Math 103B - A. Terras - Lectures #6

**FACTOR RINGS**

Building new rings from old — and generalizing $\mathbb{Z}/n\mathbb{Z}$.

Example. $\mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5$

This is a factor ring consisting of equivalence classes or cosets of integers $\text{mod } 5$. We identify $x$ and $y$ in $\mathbb{Z}$ if $x - y$ is divisible by 5, and say $x \equiv y$ (mod 5). The set of all numbers congruent to 1 (mod 5) is a coset

$$[1] = 1 + 5\mathbb{Z} = \{1 + 5y \mid y \in \mathbb{Z}\}.$$

Note $[4] = 1 + 5\mathbb{Z} = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$

So

$$[1] = [6] = \bar{-4}.$$

We add (and multiply) in $\mathbb{Z}_5$ by adding (multiplying) coset representatives, for example

$$[2] \cdot [4] = [8] = [3].$$

We get the same coset no matter what representatives we pick; for example, $[7] = \bar{2}$, $[4] = \bar{-1}$

$$\Rightarrow [7] \cdot [\bar{-1}] = [\bar{-7}] = [3].$$

Next, we want to generalize this to $R/I$, where $R =$ ring, $S \subseteq R$, $S =$ subring.

Look at $R/I$, This means
we look at cosets $a + I = \{a + b \mid b \in I\}$, or we can view $a + I = \overline{a}$ as equivalence class of $a$ under the equivalence relation on $R$ defined by $a, b \in R$

$$a \equiv b \pmod{I} \iff a - b \in I \iff a \equiv b + I = \overline{b}.$$  

Extra Credit Exercise: Show that $a \equiv b \pmod{I}$ defines an equivalence relation on $a, b \in R$ when $R = \mathbb{Z}$ and $I = n\mathbb{Z}$ show that this is congruence mod $n$.

Question: When is $R/I$ a ring under operations defined as follows for $a, b \in R$

- cosets $\overline{a} = a + I$, $\overline{b} = b + I$
- $\overline{a} + \overline{b} = \overline{a + b}$, $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$?

Answer: when $I$ is an ideal.

Define: $I \subseteq R$ is an ideal if $I \neq \emptyset$ and:

1) $I$ is an additive subgroup of $R$
2) $\forall r \in R$, $a \in I$, $ra \in I$

rae $I$ and ar $e I$.

Example: $R = \mathbb{Z}$, $I = n\mathbb{Z} = \{nr \mid r \in \mathbb{Z}\}$ is an ideal. We call $n\mathbb{Z}$ the principal ideal generated by $n$, and write $<n>$.  

\[\text{Example: } R = \mathbb{Z}, \quad I = n\mathbb{Z} = \{nr \mid r \in \mathbb{Z}\} \text{ is an ideal. }\]
Theorem. Suppose $I$ is a subring of a ring $R$.

$R/I = \text{ring} \iff I = \text{ideal in } R$

Proof.

$\Rightarrow$ We just need to see the operations defined by $\ast$ on p. 17 are well defined; that is, for $a, a', b, b' \in R$

$$\bar{a} = \bar{a'}, \quad \bar{b} = \bar{b'}$$

$$\Rightarrow \left\{ \begin{array}{l}
\bar{a} + \bar{b} = \bar{a'} + \bar{b'} \\
\bar{a} \cdot \bar{b} = \bar{a'} \cdot \bar{b'}
\end{array} \right.$$  

1. $\bar{a} + \bar{b} = \bar{a+b}$ where $\bar{a} = \bar{a'}, \quad \bar{b} = \bar{b'}$

To see $\bar{a+b} = \bar{a'+b'}$, we must show

$$(a+b) - (a'+b') \in I$$

But

$$(a+b) - (a'+b') = (a-a') + (b-b')$$

and $a-a' \in I, \quad b-b' \in I$ since $\bar{a} = \bar{a'}, \quad \bar{b} = \bar{b'}$

Now $I$ is an ideal $\Rightarrow (a-a') + (b-b') \in I$

and we're done.

2. $\bar{a} \cdot \bar{b} = \bar{a \cdot b}$ and $\bar{a'} \cdot \bar{b'} = \bar{a' \cdot b'}$

with $\frac{\bar{a}}{b} = \frac{\bar{a'}}{b'}$.

We need $a'b' - ab \in I$ to know $\bar{a \cdot b} = \bar{a'b'}$.

$$a'b' - ab = a'b' - a'b + a'b - ab = a'(b'b) + (a'-a)b$$

adding and subtracting $a'b$
since \( b' - b \in I \) and \( I = \text{ideal} \), \( a'(b' - b) \in I \).
Similarly \( a - a \in I \Rightarrow (a' - a)b \in I \),
So \( a'b' - ab \in I \) and multiplication in \( \mathbb{R}/I \) is well defined.

From the fact that \( \mathbb{R} \) is a ring, it is easy to see that \( \mathbb{R}/I \) has all the ring axioms.

The identity for \(+\) is \( \overline{0} = 0 + I = I \).
The inverse of \( \overline{a} = a + I \) under \(+\) is \( (-a) + I = -\overline{a} \).

The associative law for \(+\) is
\[
\overline{a} + (\overline{b} + \overline{c}) = \overline{a + (b + c)} = \overline{a + (b + c)}
= \overline{(a + b) + c} \leftarrow \text{using associative law in } \mathbb{R}
= \overline{a + b + c}
= \overline{(a + b) + c}
\]

The distributive laws in \( \mathbb{R}/I \) are proved similarly, using the laws in \( \mathbb{R} \).

Conversely, if \( \mathbb{R}/I \) is a ring, the multiplication of cosets defined by \( \cdot \) on p. 15 is well defined. Thus, since
\[
\overline{0} = I = 0 + I = a + I = \overline{a}, \quad \forall a \in I,
\Rightarrow \overline{r} \circ \overline{0} = \overline{r \cdot a} \quad \forall a \in I, \forall r \in \mathbb{R}
\Rightarrow \overline{0} = \overline{ra} \quad \forall a \in I, \forall r \in \mathbb{R}
\Rightarrow \overline{r} \in I \quad \forall a \in I, \forall r \in \mathbb{R}
\]
Similarly, \( \overline{0} = \overline{a \cdot r} \quad \forall a \in I, \forall r \in \mathbb{R} \Rightarrow a \cdot r \in I. \)
Example

\[ R = \text{ring} = \mathbb{R} [x] = \{ \text{polynomials } \sum_{j=0}^{n} c_j x^j, c_j \in \mathbb{R} \} \]

\[ I = (x^2 + 1) \mathbb{R} = \langle x^2 + 1 \rangle = \{ \text{principal ideal generated by } x^2 + 1 \} = \{ f(x) (x^2 + 1) \mid f(x) \in \mathbb{R} [x] \} \]

What is \( R/I \)?

Answer: We view \( I = 0 + I \) as 0.

Thus writing

\[ \emptyset = x + I \]

\[ \emptyset^2 + 1 = (x + I)^2 + 1 = (x^2 + 1) + I = I \]

\[ \emptyset^2 + 1 = 0 \quad \Rightarrow \quad \emptyset \text{ is } \emptyset \]

So \( R/I \) can be identified with \( \mathbb{C} = \text{field of complex numbers} \)

Elements are \( \frac{f(x)}{g(x)} \), \( \frac{f(x)}{g(x)} \in \mathbb{R} [x] \)

By the division algorithm for polynomials,

\[ f(x) = (x^2 + 1) q(x) + r(x) \]

where \( q(x), r(x) \in \mathbb{R} [x] \) and

degree \( r \) < degree \( (x^2 + 1) = 2 \)

or \( r \) is the 0-polynomial.

So elements of \( R/I \) look like

\[ \frac{f(x)}{g(x)} + I = \frac{r(x)}{g(x)} + I = (b x + a) + I \]

\[ R/I = \{ a + b \emptyset \mid a, b \in \mathbb{R} \}, \quad \emptyset^2 = -1 \]

See Gallian p. 236
Therefore \[ \mathbb{R}/I = \frac{\mathbb{R}[x]}{(x^2+1)\mathbb{R}[x]} \cong \mathbb{C}, \]

where \( \mathbb{C} \) is the field of complex numbers.

**Our Goal.** Replace \( \mathbb{R} \) by finite field \( \mathbb{Z}_p \), \( p \) = prime, and \( x^2+1 \) by any irreducible polynomial mod \( p \) Then apply the result to error-correcting codes.

For example, take \( p = 2 \). Then \[ x^2+1 \equiv (x+1)^2 \quad (\text{mod } 2) \]

So \( x^2+1 \) is **not** irreducible.

But \( x^2+x+1 \) is irreducible (our analogue of "prime" polynomial).

Why? It doesn't have a root \( (\text{mod } 2) \)
\[ \alpha \text{ in } \mathbb{Z}_2 \text{ with } \alpha^2 + \alpha + 1 = 0 \]
\[ \alpha = 0 \text{ says } 0^2 + 0 + 1 \equiv 1 \ (\text{mod } 2) \]
\[ \alpha = 1 \text{ says } 1^2 + 1 + 1 \equiv 3 \not\equiv 1 \ (\text{mod } 2) \]

So \((x-\alpha)\) doesn't divide \( x^2+x+1 \)

in \( \mathbb{Z}_2[x] \) for all \( \alpha \in \mathbb{Z}_2 \).

Here we use a corollary of the division algorithm for polynomials (Gallian, p. 288)
Thus \[ F_4 = \frac{\mathbb{Z}_2[x]}{(x^2 + x + 1)\mathbb{Z}_2[x]} \]

is a field with 4 elements
\[ \{0, 1, \theta, 1+\theta\} \]

where \( \theta^2 + \theta + 1 = 0 \)

Suppose \( R \) is a commutative ring!

We are using principal ideals \( \langle a \rangle \) in \( R \), meaning
\[ \langle a \rangle = \{ ra \mid r \in R \} \]

Why an ideal?

1) \( \langle a \rangle \) is an additive subgroup
\[ \forall r, s \in R \Rightarrow ra + sa = (r-s)a \in \langle a \rangle \]

2) \( \forall r \in R \), \( \forall s \in R \) \( ra + sb \) is a multiple of \( a \)

Sometimes it is useful to look at fixed \( a, b \in R \) and
\[ \langle a, b \rangle = \{ ra + sb \mid r, s \in R \} \]

Here again assume \( R \) is a commutative ring.

Gallian, pg. 29 Exercise #3 asks you to generalize this to \( \langle a_1, \ldots, a_n \rangle \).

To see you get an ideal \( \langle a, b \rangle \) check:

1) \( \langle a, b \rangle \) is a group under +
\[ (ra + sb) + (r'a + s'b) = (r-r')a + (s-s')b \in \langle a, b \rangle \]

2) \( \forall r, s, r' \in R \), we have
\[ r'(ra + sb) = (r'r)a + (r's)b \in \langle a, b \rangle \]

\[ \Rightarrow \]
Let \( R \) = commutative ring with unity \( 1 \)
\( I \) = ideal in \( R \)

When is \( R/I \) an integral domain?

Answer: Given \( a, b \in R \), we have a zero divisor
\[ \{ \overline{a}, \overline{b} = \overline{ab} = \overline{0} \} \iff \{ a \notin I, b \notin I \} \]

So \( R/I \) has no zero divisors iff \( a \in I \implies \text{either } a \in I \text{ or } b \in I \)

We call such an ideal a "prime ideal."

Example: All ideals in \( \mathbb{Z} \) are principal, i.e., of the form \( \langle n \rangle = n \mathbb{Z} \).

Proof:

\( I \subseteq \mathbb{Z} \), \( I \) = ideal, \( I \neq \emptyset \) or \( \emptyset \)

Let \( n \) = least positive element of \( I \)

\[ I = \langle n \rangle = n \mathbb{Z} \]

Proof: \( m \in I \iff m = nq + r, \ 0 \leq r < n \)

\[ r = m - nq \in I \]

But \( n \) = least positive elt. of \( I \)

\[ r = 0 \]

\[ m = nq \in n \mathbb{Z} \]

\[ I \subseteq \langle n \rangle \] and clearly \( \langle n \rangle \subseteq I \)

\[ I = \langle n \rangle \]
Which \( \langle n \rangle \subseteq \mathbb{Z} \) are prime ideals?

**Answer:** \( \langle n \rangle \) with \( n = \pm \text{prime #} \), for \( ab \in \langle n \rangle \Leftrightarrow n \mid ab \)
\[ n \mid ab \Rightarrow n \mid a \text{ or } n \mid b \]

\( \Rightarrow \) means \( n = \pm \text{prime} \).

For \( n = ns, \; r, s \in \mathbb{Z} \Rightarrow n = rs \mid rs = r \cdot (rs) \cdot \text{but } n = (rs) \not\mid r \).
\[ \Rightarrow n = \pm \text{prime} \]

\( \Leftarrow \) \( n = \text{prime } \& n \mid ab \Rightarrow n \mid a \text{ or } n \mid b \)

Euclid's Lemma

But we really want \( R/I = \text{field} \).
What ideals \( I \) do this when \( R \) is a commutative ring with unity?

**When is \( R/I \) a field?**

**Answer:** I must be a maximal ideal meaning
\[ I \subseteq A \subseteq R, \; A = \text{ideal } \Rightarrow A = I \text{ or } A = R, \]

**Proof:**

\( \Rightarrow \) Suppose \( R/I = \text{field} \).
To see why I must be a maximal ideal, suppose \( I \subset B \subset R \) for some ideal \( B \) and \( B \neq I \), then \( \exists b \in B \) b \notin I.
Now $b \notin I$
$\Rightarrow \bar{b} \neq 0$ in $R/I$ a field
$\Rightarrow \exists \bar{c} \in R/I$ so that $\bar{c} \cdot \bar{b} = \bar{1}$
$\Rightarrow x = cb - 1 \in I \Rightarrow 1 = cb - x \in B \subseteq B I C B$
$\Rightarrow B = R$ as $1 \in B \Rightarrow r \cdot 1 = r \in B \forall r \in R$
So $I$ is maximal.

Conversely, if $I$ is a maximal ideal in $R$, let $b \in R$, $\bar{b} \neq 0 \in R/I \iff b \notin I$.
Look at ideal $B$ generated by $I$ and $b$, that is
$B = \{ a + rb \mid a \in I, \, r \in R \}$

**Extra Credit Exercise**
Show $B$ is an ideal.

Since $I \subseteq B$, we know $B = R$
So $1 = a + rb$, for some $a \in I, \, r \in R$
$\Rightarrow \bar{1} = \bar{r} \cdot \bar{b}$
Thus $\bar{r} = \bar{b}^{-1}$ and $R/I$ is a field.
Example \( \text{In } \mathbb{Z} \text{ what are the maximal ideals?} \)

We know all ideals of \( \mathbb{Z} \) are principal that is of the form \( \langle n \rangle = n \mathbb{Z} \).

If \( \langle n \rangle = n \mathbb{Z} \) is maximal, \( \mathbb{Z} / n \mathbb{Z} = \mathbb{Z}_n \) is a field, as we just proved.

But we know (Gallian, p. 251) \( \mathbb{Z}_n \) is a field \( \iff n = \text{prime} \). Thus, in \( \mathbb{Z} \) maximal ideals are \( \langle p \rangle = p \mathbb{Z} \), \( p = \text{prime} \).

And maximal ideals are the same in \( \mathbb{Z} \) as prime ideals.

Example \ Find all the maximal ideals in \( \mathbb{Z}_{12} \). \ To do this you just need to see all ideals \( I \) in \( \mathbb{Z}_{12} \) are principal as the correspond to ideals \( \tilde{I} \) in \( \mathbb{Z} \):

\[
\tilde{I} = \{ m \in \mathbb{Z} | m \equiv n \pmod{12} \} \text{ in } I
\]

We know \( \tilde{I} = \langle n \rangle \) for some \( n \in \mathbb{Z} \).

So \( I = \langle n \rangle \) in \( \mathbb{Z}_{12} \).
Next note if $\mu$ is a unit in $\mathbb{Z}_{12}$
$\mu \mu^{-1} = 1 \pmod{12}$, so
\[ < \mu \nu > = < \nu > \text{ in } \mathbb{Z}_{12}. \]

Thus ideals in $\mathbb{Z}_{12}$ are
\[ < 0 >, < 1 > = \mathbb{Z}_{12}, < 2 > = \{ 2x \mid x \in \mathbb{Z}_{12} \} = \{ 0, 2, 4, 6, 8, 10 \} \pmod{12} \]
\[ < 3 > = \{ 0, 3, 6, 9 \} \pmod{12}, < 4 > = \{ 4x \mid x \in \mathbb{Z}_{12} \} = \{ 0, 4, 8 \} \pmod{12} \]
\[ < 5 > = < 1 > = < 7 > = < 11 > = \mathbb{Z}_{12}, < 6 > = \{ 0, 6 \} \pmod{12} \]
\[ < 8 > = \{ 8x \mid x \in \mathbb{Z}_{12} \} = \{ 0, 8 \} \pmod{12} \]
\[ < 9 > = \{ 9x \mid x \in \mathbb{Z}_{12} \} = \{ 0, 9, 6, 3 \} \pmod{12} = < 3 > \]
\[ < 10 > = < 2 > \]

The lattice of ideals in $\mathbb{Z}_{12}$ is:
$\mathbb{Z}_{12} = < 1 > = < 5 > = < 7 > = < 11 >$

\[ < 2 > = < 10 >, < 3 > = < 9 >, < 6 > \]
\[ < 8 > \]
\[ < 0 > \]

So the maximal ideals in $\mathbb{Z}_{12}$ are $< 2 >$ and $< 3 >$. 

You may wonder why \( \langle 8 \rangle = \langle 4 \rangle \) in \( \mathbb{Z}_{12} \).

It is not hard to see why

\[
\langle 8 \rangle = \{ 8 \cdot x \mid x \text{ mod } 3 \} = \langle 4 \rangle = \{ 4 \cdot y \mid y \text{ mod } 3 \}
\]

\[
8x = 4y \quad (\text{mod } 12)
\]

\[
\Rightarrow 2x = y \quad (\text{mod } 3)
\]

This has a unique solution \( x \) (mod 3) for each \( y \) corresponding to a unique \( 8x \) for each \( 4y \) (mod 12).

**Gallian, Problem #4, p. 269**

We need a subring \( S \subset R = \mathbb{Z} \oplus \mathbb{Z} \), that is not an ideal.

Recall \( \mathbb{Z} \oplus \mathbb{Z} \) is the set of \( (a, b), a, b \in \mathbb{Z} \) with \( (a, b) + (a', b') = (a+a', b+b') \) and \( (a, b) \cdot (a', b') = (a \cdot a', b \cdot b') \).

Try:

\[
S = \{ (a, b) \mid a, b \in \mathbb{Z}, a+b \text{ even } \}
\]

It isn't too hard to show \( S \) is an additive subgroup.

Why closed under multiplication?

\[
\text{a+b even and a'+b' even } \Rightarrow 2(aa' + bb') = (a+b)(a'+b') - (a-b)(a'-b')
\]

Now 4 divides the right-hand side.

So 2 divides \( aa' + bb' \).
So $S$ is a subring of $R$. To see that $S$ is not an ideal, look at

$(1, 3) \in S$ and $(1, 0) \in R$.

Then $(1, 3)(1, 0) = (1, 0) \notin S$.
So $S$ is not an ideal.