Quiz Friday: convergence of sequences, Cauchy sequences, homomorphisms, isomorphisms.

Last time: subrings, homomorphisms, isomorphisms.

Recall a subset $S$ of a ring $R$ is a subring if

(i) $0 \in S$  
(ii) $s, t \in S \Rightarrow s + t, st \in S$  

Then $(S, +, \cdot, 0_{R})$ is a ring.

Note we need (i) and (ii): $\mathbb{N}$ is not a subring of $\mathbb{Z}$, but $\mathbb{N} \subseteq \mathbb{Z}, a + b, a \cdot b \in \mathbb{N}$.

Lemma 19.1 Suppose $R$ is a ring, $S \subseteq R$ a subset so that

(i) $s, t \in S$, $s + t \in S$ and $s \cdot t \in S$.

(ii) Since $S + 0_{R} = S$ then $0_{R} - S = S'$.

(iii) $s, t \in S$, $-t \in S \Rightarrow S + (-t) = S - t \subseteq S$.

Proof: We argue that (i) $0 \in S$, (ii) $s, t \in S$, $s - t \in S$.

(i) Since $S + 0_{R} = S$ then $0_{R} - S = S'$.

(ii) $s, t \in S$, $0_{R} - S$ since $0_{R} \in S'$.

(iii) $s, t \in S$, $-t \in S \Rightarrow S + (-t) = S - t \subseteq S$.

Lemma 19.2 Suppose $f: R \rightarrow S$ is a homomorphism.

Then $f(R) = \{ f(r) \mid r \in R \}$ is a subring of $S$.

Moreover, if $f(1_{R}) = 1_{S}$ then $f(R)$ has $1_{S}$.

Proof: $f(R) \neq \emptyset$, since $R \neq \emptyset$.

(i) If $x, y \in f(R)$ then $x = f(a), y = f(b)$ for some $a, b \in R$.

$\Rightarrow x \cdot y = f(a) \cdot f(b) = f(ab) = f(R)$

$x - y = f(a) - f(b) = f(a + (-b)) = f(R)$.

$\Rightarrow f(R)$ is a subring by 19.1.

We've seen: the set $\text{Map}(\mathbb{N}, \mathbb{R})$ of all sequences $\mathbb{N} \rightarrow \mathbb{R}$ is a ring.

Let $C = \{ g \in \text{Map}(\mathbb{N}, \mathbb{R}) \mid \text{for all } i \text{ is Cauchy } g \}$.

Goal: $C$ is a subring of $\text{Map}(\mathbb{N}, \mathbb{R})$ hence a ring.
We need first

Sally, Lemma 3.5.7 If \( \{a_n\} \subset \mathbb{Q} \) is Cauchy then \( \exists M \in \mathbb{Q} \)

so that \( |a_n| \leq M \) \( \forall n \)

ie. \( \{a_n\} \) is bounded.

Proof Fix \( \varepsilon = 1 \). \( \exists N \in \mathbb{N} \) st. for \( n, m \geq N \)

\[ |a_n - a_m| < 1 \]

Let \( M = \max \{ |a_1|, \ldots, |a_N|, |a_N + 1| \} \)

If \( k \leq N \) then \( |a_k| \leq M \). (by definition of \( M \))

If \( k > N \), \( |a_k| = |a_k - a_N + a_N| \leq |a_k - a_N| + |a_N| \leq |a_N + 1| \leq M \).

---

**Lemma 19.3** The set \( \mathbb{Q} \) of Cauchy sequences in \( \mathbb{Q} \) is a subring of \( \operatorname{Map} (\mathbb{N}, \mathbb{Q}) \) (containing 1). 

Proof (i) Any constant sequence is Cauchy.

So in particular the sequence \( a_n = 1 \) \( \forall n \) is Cauchy.

(ii) Suppose \( \{a_n\}, \{b_n\} \in \mathbb{Q} \). We argue: \( |a_n - b_n| = |a_n - b_0 + b_0 - b_n| \)

Fix \( \varepsilon > 0 \). Then \( \exists N_1, N_2 \) so that

\[ \forall n, m > N_1 \quad |a_n - a_m| < \frac{\varepsilon}{2} \]

\[ \forall n, m > N_2 \quad |b_n - b_m| < \frac{\varepsilon}{2} \]

\[ a_n, a_m, b_n, b_m \text{ in Cauchy.} \]

Next we argue: \( |a_n - b_n| = |a_n - b_0 + b_0 - b_n| \)

Since \( \{a_n\}, \{b_n\} \) are Cauchy, they are both bounded. \( \forall A, B \in \mathbb{Q} \)

\[ |a_n| \leq A \quad \forall n, \quad |b_n| \leq B \quad \forall n. \]

Now given \( \varepsilon > 0 \), \( \exists N_1, N_2 \) st. for \( n, m > N_1 \)

\( |a_n - a_m| < \frac{\varepsilon}{2B} \)

\( |b_n - b_m| < \frac{\varepsilon}{2A} \)

Therefore for \( n, m > \max \{ N_1, N_2 \} \)

\( |a_n b_n - a_m b_m| = |a_n b_n - a_n b_m + a_n b_m - a_m b_m| \)

\[ \leq |a_n||b_n - b_m| + |a_n - a_m||b_m| < A \cdot \frac{\varepsilon}{2B} + B \cdot \frac{\varepsilon}{2A} = \varepsilon. \]
By lemma 19.1, \( \mathbb{E} \) is a subring of \( \text{Map}(\mathbb{N}, \mathbb{E}) \) (containing \( 1 \)), hence a ring with 1. 

---

**Definition**

Let \( R \) be a commutative ring.

A nonempty subset \( I \) of \( R \) is an ideal if:
1. \( \forall a, b \in I \) \( a - b \in I \)
2. \( \forall r \in R \) \( r \cdot a \cdot I \cdot r \cdot a \in I \).

For example, \( R = \mathbb{Z} \), \( n \mathbb{Z} = \{ nk | k \in \mathbb{Z} \} \) is an ideal in \( \mathbb{Z} \):

- \( \forall a, b \in \mathbb{Z} \), \( a = nk_1, b = nk_2 \) for some \( k_1, k_2 \in \mathbb{Z} \)
- \( a - b = n(k_1 - k_2) \in n \mathbb{Z} \)

Note: \( \mathbb{Z} \subseteq \mathbb{Q} \) is a subring but not an ideal.

**Note:** If \( R \) is a ring with 1, \( I \subseteq R \) an ideal and \( 1 \in I \) then \( I = R \).

**Reason:** \( \forall r \in R, r \cdot 1 \cdot I \in I \) since \( 1 \in I \).

If we want "interesting" ideals they should not have 1.

**Road Map.** An ideal \( I \subseteq R \) defines an equivalence relation \( \sim \) on \( R \). The set \( R/\sim \) of equivalence classes is naturally a ring.

**Lemma 19.4** Let \( I \) be an ideal in a commutative ring \( R \).

The relation \( \sim \) defined by
\[
\forall a, b \in I \quad a \sim b \iff a - b \in I
\]
is an equivalence relation.

**Proof:** (i) Since \( I \neq \emptyset \) there exists \( x + I \). Then \( \emptyset = x - x + I \).

\( \forall r \in R, r \cdot \emptyset \) since \( 1 - 1 = 0 \in I \).
(ii) Since $0 \in I$, $\forall x \in I$, $0-x = -x \in I$. 
Now suppose $r \sim r'$. Then $r-r' \in I$. \[ I \ni -(r-r') = r'-r \sim r. \]

(iii) If $x, y \in I$, $y \in I$. \[ x+y = x-(-y) \in I \]
Now suppose $x \sim y$, $y \sim z$. Then $x-y, y-z \in I$\[ I \ni (x-y)+(y-z) = x-y+y-z = x-z. \]
\[ \Rightarrow x \sim z \]
\[ \therefore \sim \text{ is an equivalence relation.} \]

Example If $R = \mathbb{Z}$, $I = n\mathbb{Z}$, $m \sim m' \Leftrightarrow m-m' \in n\mathbb{Z}$\[ \Leftrightarrow n \mid (m-m') \]
The set $R/I$ of equivalence classes in $\mathbb{Z}_n$.

In general, given an ideal $I \subset R$, \[ r+I = \{ r' \mid r \sim r', r' \in I \} \]
\[ = \{ r' \mid r' = r+i \text{ for some } i \in I \} = \{ i \in I \} = : r+I. \]

Notation $R/I = \{ r+I \mid r \in R \}$ the set of equivalence classes in the ring $R$ defined by the ideal $I$.

Remarks

(1) $0 \subseteq I$ and $R$ are ideals in a ring $R$.

(2) If $R$ is a field, $0 \subseteq I$ and $R$ are the only ideals:
If $I \subset R$ is an ideal and $I \neq 0$, \[ \exists a \in I, a \neq 0. \]
Since $R$ is a field, $a$ has a multi-inverse $a^{-1}$.
\[ 1 = a^{-1}a \in I. \]
\[ \Rightarrow R \subseteq I \text{ (as we've seen above)} \]
\[ \therefore R = I. \]

Next time $R/I$ is a ring (just like $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ is a ring).