Day 12

Ring homomorphisms

Some example computations with ideals and quotient rings

- ideals of $\mathbb{Z}$ and quotients
- ideals $(x^2+1)R$ of $R = \mathbb{Q}[x]$, $R = \mathbb{R}[x]$, and $R = \mathbb{C}[x]$
- Ring of functions $X \to A$ and the evaluation map at points of X.
- Evaluation map on polynomials $R[x] \to S$ extending $R \to S$ given by evaluation at $s \in S$.
- $\mathbb{Z}/p\mathbb{Z}[x]/(f(x))$
- $\mathbb{Z}[i]/2$, $\mathbb{Z}[i]/3$, $\mathbb{Z}[i]/5$
- two sided ideals of $M_n(R)$
- examples of left ideals of $M_n(R)$.

Isomorphism theorems

1. R a ring, A a subring, and B and ideal of R. Let $A+B = \{a+b | a \in A, b \in B\}$. Then $A \cap B$ is an ideal of A and $(A+B)/B \cong A/(A \cap B)$.
2. If I and J are ideals of R and $I \subset J$, then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.
3. Let $I \subset R$ be an ideal. There is a bijective correspondence $A \to A/I$ between subrings of R containing I and subrings of R/I. This correspondence respects ideals, so A/I is an ideal of R/I if and only if A is an ideal of R.

Sums and products of ideals

1. The sum $I+J$ of two ideals is the collection of sums of elements of I and J; it is an ideal.
2. The product IJ is the subring generated by products ab with $a \in I$ and $b \in J$; it is an ideal.
3. I^n is the product of I with itself n times. it is an ideal.

Prime and maximal ideals

Suppose that R has an identity element 1 (and that 1 is not zero, so the ring is not trivial).

- An ideal $I = R$ if and only if I contains a unit.
- R is a field iff its only ideals are zero and R.
- Any homomorphism from a field F to another ring R is either zero or injective.

Maximal ideals and Zorn's lemma

Definition: A *partial order* on a set A is a relation $\leq$ on A such that is reflexive (so $a \leq a$ for all $a \in A$), antisymmetric (so $a \leq b$ and $b \leq a$ implies $a = b$) and transitive (so $a \leq b$ and $b \leq c$ implies $a \leq c$).

Definition: A *total order* on A is a partial order with the additional property that, given $a, b \in A$, either $a \leq b$ or $b \leq a$.

Definition: A *chain* in A is a subset of A which is totally ordered by $\leq$.

Definition: An upper bound for a subset B of a partially ordered set A is an element $a \in A$ such that, for all $b \in B$, $b \leq a$.

Definition: A maximal element of a partially ordered set A is an element $m \in A$ such that $m \leq x \implies m = x$ for all $x \in A$.

Examples:

- integers under divisiblity are partially ordered; powers of a prime p are chains.
- subsets of a set X under inclusion are partially ordered; a chain is a nested sequence of sets. The union of elements in a chain is an upper bound for the chain. The whole set X is a maximal element.
- Let A be the set of pairs (X, f) where $X \subset \mathbb{R}$ is open and $f : X \to \mathbb{R}$ is continuous (or differentiable, $\ldots$). The relation $(X, f) \leq (Y, g)$ if $X \subset Y$ and g restricted to X is f.

Zorn's Lemma: If A is a *nonempty* partially ordered set in which *every chain has an upper bound* then A has a maximal element.

Not a lemma – really an axiom.

If R is a ring with unity, let J be a proper ideal of R and let A be the set of proper ideals of R containing J. Then A satisfies the conditions of Zorn's lemma – a chain is an increasing system of proper ideals; the union of proper ideals is a proper ideal (if the union weren't proper, it would contain 1, so 1 would belong to one of the elements in the sequence, which can't happen); that union is the upper bound for that chain. So A has a maximal element which is a proper ideal containing J.

Proposition: (Krull) Every ideal in a ring with unity is contained in a maximal ideal.