Day 13

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.

Decomposition of rings

Suppose R is **a commutative ring with unity.**

Definition: Two ideals I and J of a ring R are called coprime or comaximal if $I + J = R$.

Lemma: If $I + J = R$ then $IJ = I \cap J$.

Proof: We know $IJ \subset I \cap J$. Choose $x \in I \cap J$ and also write $1 = u + v$ with $u \in I$ and $v \in J$. Then $x = xu + xv$. But both xu and xv are in IJ, so $x \in IJ$.

This is a (pretty big) generalization of the statement that if a and b are relatively prime integers then their least common multiple is their product.

Proposition: Let $I_1, \ldots, I_k$ are ideals of R, then there is a ring homomorphism

$$R \to R/I_1 \times \cdots \times R/I_k.$$

Its kernel is the intersection $\bigcap_{i=1}^{k} I_i$. If, for every pair, $I_j + I_k = R$, the map is surjective and its kernel is $I_1 \cdots I_k$.

Key examples: Polynomials and integers.

Ideals and divisibility

Euclidean Domains

Three notable examples:

- $\mathbb{Z}$
- $F[x]$ where F is a field
- $\mathbb{Z}[i]$

Proposition: Every ideal in a Euclidean domain is principal.

Proposition: (Fermat) A prime number is the sum of two squares if and only if it is 2 or is congruent to 1 mod 4.

Lemma: The congruence $x^2 \equiv -1 \pmod{p}$ has a solution modulo a prime p if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

Proof: If $p = 2$, 1 is a solution. If p is odd, and $x^2 = -1$ has a solution, then $(\mathbb{Z}/p\mathbb{Z})^*$ has an element of order 4, so $4|(p-1)$. Notice that $(\mathbb{Z}/p\mathbb{Z})^*$ has only two elements of order dividing 2, because of $x^2 \equiv 1 \pmod{p}$ then $p|(x^2-1)$, so $p|(x+1)(x-1)$, so either $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. If $4|(p-1)$ then let H be the Sylow 2-subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$. If H were not cyclic, then there would be too many elements of order 2 in H. So H must be cyclic and therefore there is an element of order 4.

Now suppose that $p \equiv 1 \pmod{4}$. Let u be a solution to $x^2 + 1 \equiv 0 \pmod{p}$. Consider the ideal $I = (p, u + i) \subset \mathbb{Z}[i]$. This is a maximal ideal. If $\pi = a + bi$ is a generator of this ideal, then $p = x\pi$. If x were a unit, then $u + i$ would have to be a multiple of p, which it visibly isn't. Therefore $N(\pi)$ must be p. But $N(\pi) = a^2 + b^2$, so we've found our representation.