Course Overview:

1. "Nice" rings and factorization.
   
   Ring: Let $R$ be a ring with $+, \times$. $[\langle R, + \rangle]$ is a group, $\times$ is associative.

   Suppose $R$ is commutative, has 1, no zero divisors.

   Ex: $\mathbb{Z}, \mathbb{R}, \mathbb{Z}[x] \ldots$ [Query for more]

   $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$
   
   $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$. primes

   Any $n \in \mathbb{Z}$ can be written $n = (\pm 1) p_1 \ldots p_k$

   Units in $R$: those elts with multi. inverses.
   Inreducible: if $r = a \cdot b$ then one of $a, b$ is a unit.

   Unique factorization: Any $r \in R$ is $r = r_1 \cdot r_2 \ldots r_n$, where $r_i$ inreducible, in an essentially unique way.

   Ex: $6 = 2 \cdot 3 = 3 \cdot 2 = (-3)(-2) = (-2)(-3)$. 
\textbf{Fact:} \( \mathbb{Z}[i] \) has unique factorization, but \( \mathbb{Z}[\sqrt{5}i] = \mathbb{Z}[\sqrt{-5}] \) doesn't!

\[ 6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 1 + 5 = 6. \]

\[ \uparrow \quad \uparrow \quad \text{all } \in \mathbb{Z} \] (HW)

\textbf{Motivation:} Many elem. facts about number theory can be understood in terms of factoring in certain rings. E.g.

\textbf{Thm:} An odd prime \( p \) in \( \mathbb{Z} \) is \( a^2 + b^2 \) (for \( a, b \in \mathbb{Z} \)) iff \( p = 1 \mod 4. \)

\[ \text{[Goes back to the ancient Greeks: "best" understood in terms factorization in } \mathbb{Z}[i]. \]

\textbf{Euclidean Domain} \Rightarrow \text{Principal ideal Domain} \Rightarrow \text{Unique Factorization}

\textbf{Aside:} Restoring unique factorization leads to ideals = "Ideal numbers".

\textit{Fermat's Last Thm:} \( a^n + b^n = c^n \) has no solutions for \( a, b, c \in \mathbb{Z} \) nonzero + \( n \geq 3. \)

\textit{Proved by} Wiles in early 1990s.
2 Galois Theory

Broadly, the study of field extensions $F \subseteq K$

$\text{Ex: } R \subseteq C, \ Q \subseteq Q(\sqrt{2}) \subseteq Q(\sqrt{2}, \sqrt{3}) \subseteq C$

\uparrow \text{alg. extension, adding roots of a poly.}

$Q \subseteq Q(\pi)$ focus of Galois theory

\downarrow \text{transcendental extension}

Given $F \subseteq K$ an alg. extension, get associated finite group $\text{Gal}(K/F)$.

$\text{Ex: } \text{Gal}(Q(\sqrt{2}, \sqrt{3})/Q) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

When $K/F$ is Galois (whatever that means...)
then subfields $F \subseteq L \subseteq K$ correspond to subgroups to $\text{Gal}(K/F)$.

Query: How many subgroups of $(\mathbb{Z}/2\mathbb{Z})^2$ are there?  A. 5

Much of finite group theory was developed to study Galois groups.
Applications: 1. Unsolvability of the general quintic.
   2. Can't trisect an angle.

Other topics: 1. Algebraic geometry?
   2. Error correcting codes?
   3. Representation theory of finite groups?

Go over syllabus.