In order to solve Fermat’s last conjecture, Kummer worked with the ring \( \mathbb{Z}[\zeta_n] = \{ \frac{a_0}{n} \zeta_n + \frac{a_1}{n^2} \zeta_n^2 + \ldots + \frac{a_{n-1}}{n^{n-1}} \zeta_n^{n-1} \mid a_i \in \mathbb{Z} \} \) where \( \zeta_n = e^{2 \pi i / n} \). He realized that in this ring, numbers might be written as products of prime in different ways. But when he worked with “ideal numbers”, he could write them as product of “prime ideal number” in a unique way. Later Dedekind and Noether extended these concepts to all rings; and now we talk about ideals and prime ideals.

**Def.** Suppose \( R \) is a ring. We say \( I \subseteq R \) is an ideal if

1. \( I \) is a subring, 2. \( \forall r \in R, \forall a \in I, ra \in I \) and \( ar \in I. \)

We write \( I \triangleleft R. \)

**Lemma.** Suppose \( R \) is a ring and \( \varnothing \neq I \subseteq R. \) Then \( I \triangleleft R \) if and only if

1. \( \forall a, b \in I, a - b \in I \) 2. \( \forall a \in I, r \in R, ra \in I. \)

**Pr.** \((\Rightarrow)\) Since \( I \) is a subring, (1) holds; since \( I \triangleleft R \), (2) holds.

\((\Leftarrow)\) We only need to say why \( I \) is a subring. By the subring
criterion it is enough to show $\forall a, b \in I$, $a - b \in I$ and $ab \in I$;

And both are direct consequences of our assumptions. $\blacksquare$

**Ex.** $I \triangleleft \mathbb{Z} \iff I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

**Proof.** ($\Rightarrow$). $a, b \in \mathbb{Z} \implies n \mid a, n \mid b \implies n \mid a - b \implies a - b \in n\mathbb{Z}$.

* $a \in n\mathbb{Z}$ $\implies \exists n \mid a$ $\implies n \mid ar$ and $n \mid ra$ $\implies r \in n\mathbb{Z}$.

($\Leftarrow$). If $I = 0$, we are done.

If $I \neq 0$, let $n \in I \setminus \{0\}$. Then $n \in I$. And so $I$ has a positive integer. Let $n_0 = \min I \cap \mathbb{Z}^+$. Then $n_0 \mathbb{Z} \subseteq I$.

**Claim.** $n_0 \mathbb{Z} = I$.

**Proof of claim.** For me $I$, by the division algorithm, $\exists q, r \in \mathbb{Z}$ s.t. $m = n_0q + r$, $0 \leq r < n_0$.

And so $r = m - n_0q \in I \cap [0, n_0 - 1)$ $(\star)$

Since $n_0 = \min I \cap \mathbb{Z}^+$, by $(\star)$ $r = 0$. And so $m = n_0q \in n_0 \mathbb{Z}$. $\blacksquare$
Lecture 08: Finitely generated Ideals

We say \( I \) is the ideal generated by \( a_1, \ldots, a_n \) if \( I \) is the smallest ideal of \( R \) that contains \( a_1, \ldots, a_n \). We denote it by \( \langle a_1, \ldots, a_n \rangle \).

Claim. \( \langle a_1, \ldots, a_n \rangle = \{ \sum r_i a_i \mid r_i \in R \} \).

Proof. Let's call the right hand side by \( J \).

Step 1. If \( I \triangleleft R \) and \( a_1, \ldots, a_n \in I \), then \( J \subseteq I \).

Proof. \( a_i \in I \Rightarrow \forall r_i \in R, r_i a_i \in I \)

\( \Rightarrow \sum r_i a_i \in I \). And so \( J \subseteq I \).

Step 2. \( J \triangleleft R \).

Proof. \( \left( \sum_{i=1}^{n} r_i a_i \right) - \left( \sum_{i=1}^{n} r'_i a_i \right) = \sum_{i=1}^{n} (r_i - r'_i) a_i \in J \).

\( \forall r \in R, r \left( \sum_{i=1}^{n} r_i a_i \right) = \sum_{i=1}^{n} r r_i a_i \in J \).

Since \( R \) is commutative,

\( \left( \sum_{i=1}^{n} r_i a_i \right) r = r \left( \sum_{i=1}^{n} r_i a_i \right) \in J \).

Step 3. \( a_1, \ldots, a_n \in J \).

Proof. Since \( R \) is unital, \( 1 a_i = a_i \in J \).
An ideal is called principal if it is generated by 1 element.

An integral domain is called a Principal Ideal Domain (PID) if any ideal is principal.

**Ex.** \( \mathbb{Z} \) is a PID.

**Lemma.** Suppose \( f : R_1 \rightarrow R_2 \) is a ring homomorphism. Kernel of \( f \) is \( \ker f = \{ r \in R_1 \mid f(r) = 0 \} \). Then \( \ker f \triangleleft R_1 \).

**Pf.** \( a, b \in \ker f \Rightarrow f(a) = 0, f(b) = 0 \)

\[ \Rightarrow f(a-b) = f(a) - f(b) = 0 \]

\[ \Rightarrow a-b \in \ker f. \]

\( a \in \ker f, r \in R \Rightarrow f(ar) = f(a) f(r) = 0 \cdot f(r) = 0 \)

\[ \Rightarrow ar \in \ker f. \]

Similarly \( f(ra) = f(r) f(a) = f(r) \cdot 0 = 0 \Rightarrow ra \in \ker f. \)

And so \( \ker f \triangleleft R_1. \)

Using an ideal we can construct a new ring; that is called the factor ring of \( R \) by \( I \) and it is denoted by \( R/I \).
Proposition. Suppose \( I \triangleleft R \). Let \( R/I := \{ r+I \mid r \in R \} \) be the set of all the (additive) cosets of \( I \) in \( R \). Then 

\[(R/I, +, \cdot)\] is a ring where

- \((a+I) + (b+I) = (a+b) + I\),

- \((a+I)(b+I) := ab + I\).

(We will continue next time.)