Recall in the previous lecture:

Definition 1. An *ideal* in a ring R is a subring $I \lhd R$ such that if $a \in I$ and $r \in R$, then $ar, ra \in I$.

Observe that if $I \leq R$, then

- $(R, +)$ is an abelian group and $(I, +) \leq (R, +)$ and for $r \in R$, then $r + I = I + r$. This is what it means for $I \lhd R$ to be a normal subgroup.

Definition 2. The set
$$R/I = \{r + I : r \in R\}$$
is called the *factor ring* or *quotient ring.*

Based on the definition above, we note that R/I is a group with addition and operation defined by
$$(r + I) + (s + I) = (r + s) + I$$
For the multiplication, we seek an operation so that R/I under multiplication is well defined.

Lemma 1. *Let $I \leq R$. Then the operation $(r+I)(s+I) = (rs)+I$ is well defined if and only if $I \lhd R$.*

Proof. Suppose that $I \lhd R$. We want to show that for all $a, b \in I$,
$$(r + I)(s + I) = [(r + a) + I][(s + b) + I]$$
So on the right hand side, we have
$$\begin{aligned}[(r + a) + I][(s + b) + I] &= (r + a)(s + b) + I \\ &= (rs + as + rb + ab) + I \\ &= (rs) + I\end{aligned}$$

On the other hand, assume that $I \leq R$. Then there exists an $r \in R$ and $a \in I$ such that either $ar \notin I$ or $ra \notin I$, or both. Without loss of generality, assume that $ar \notin I$. Then
$$(0 + I)(r + I) = 0r + I = 0 + I$$
but
$$(a + I)(r + I) = ar + I$$
But $ar \notin I$, so $ar + I \neq 0 + I$. Therefore, the operation is not well defined. $\square$

Example 1. • For $n \in \mathbb{N}$, $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\langle n \rangle$.

- How many elements does $\mathbb{Z}[x]/\langle x, 2\rangle$ have? Note that

$$\langle x, 2\rangle = \{xg(x) + 2f(x) : f(x), g(x) \in \mathbb{Z}[x]\}$$

  Let $p(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{Z}[x]$, then $f(x) \in \langle x, 2\rangle$ if c_0 is even, and $f(x) \in \langle x, 2\rangle$ if c_0 is odd.

Recall that if $\phi : R \to S$ is a ring homomorphism, the kernel of ϕ is an ideal of R.

Theorem 1. *Let $I \lhd R$. Then the map $\phi : R \to R/I$ defined by $\phi(r) = r + I$ is a ring homomorphism from R to R/I and $\ker(\phi) = I$.*

Theorem 2 (First Isomorphism Theorem)**.** *Let $\psi : R \to S$ be a ring homomorphism. Then $\ker(\psi)$ is an ideal of R. If $\phi : R \to R/\ker(\psi)$ is the canonical homomorphism, then there exists a unique isomorphism $\eta : R/\ker(\phi) \to \psi(R)$ such that $\psi = \eta\phi$.*

Example 2. Consider the evaluation homomorphism $\phi_\alpha : \mathbb{Z}[x] \to \mathbb{Z}$ given by $\phi_\alpha(f(X)) = f(\alpha)$. Then

$$\ker(\phi_\alpha) = \langle x\rangle$$

and so by the first isomorphism theorem, $\mathbb{Z}[x]/\langle x\rangle \simeq \phi_\alpha(\mathbb{Z})$. We want to show that $\phi_\alpha(\mathbb{Z}[x]) = \mathbb{Z}$, or ϕ_α is onto. For all $a \in \mathbb{Z}$, let $f(x) = a$ and $\phi_\alpha(f(x)) = a$, so ϕ_α is onto so $\mathbb{Z}/\langle x\rangle \simeq \mathbb{Z}$.