LECTURE 8.

ALIREZA SALEHI GOLSEFIDY

Last time we saw the definition of the ideal generated by a given subset $X$ of $R$. We also saw that if $R$ is a unital commutative ring then

$$\langle a_1, \ldots, a_n \rangle = \{ \sum_{i=1}^n r_i a_i | r_i \in R \}.$$ 

The following lemma shows what happens if we drop the unital and commutativity conditions:

**Lemma 1.** For an arbitrary ring $R$, the ideal generated by $a$ is

$$\langle a \rangle = \{ \sum_{i=1}^m r_i a'_i + ra + ar' + na | n \in \mathbb{Z}, r, r', r_i, r_i' \in R \}.$$ 

**Proof.** It follows from the properties of an ideal. $\square$

Last time we also saw that any ideal of $\mathbb{Z}$ is generated by one element.

**Definition 2.**

1. If $X = \{ a \}$, then $\langle X \rangle$ is often denoted by $\langle a \rangle$ and it is called a principal ideal.
2. A ring $R$ is called a principal ideal ring (PIR) if $R$ is non-zero commutative unital ring all of whose ideals are principal.
3. A PIR is called a principal integral domain (PID) if it is also an integral domain.

**Example 3.** $\mathbb{Z}$ is a PID.

**Lemma 4.** Let $f : R \to S$ be an onto ring homomorphism. If $I$ is an ideal of $S$, then

1. the preimage of $I$ is an ideal of $R$.
2. $\ker(f) \subseteq f^{-1}(I)$.
3. $f(f^{-1}(I)) = I$.
4. There is a bijection between the ideals of $R$ which contains $\ker(f)$ and the ideals of $S$:

$$\{ I \mid I \trianglelefteq S \} \overset{f^{-1}}{\rightarrow} \{ J \trianglelefteq R \mid \ker(f) \subseteq J \}.$$ 

**Proof.** 1. To prove that $f^{-1}(I)$ is an ideal, we have to check the following: $f^{-1}(I) - f^{-1}(I) \subseteq f^{-1}(I)$, $Rf^{-1}(I) \subseteq f^{-1}(I)$ and $f^{-1}(I)R \subseteq f^{-1}(I)$.

$$r_1, r_2 \in f^{-1}(I) \Rightarrow f(r_1), f(r_2) \in I$$
$$\Rightarrow f(r_1 + r_2) = f(r_1 - r_2) \in I$$
$$\Rightarrow r_1 - r_2 \in f^{-1}(I).$$

For any $r \in R$ and $r' \in f^{-1}(I)$, we have

$$r' \in f^{-1}(I) \Rightarrow f(r') \in I$$
$$\Rightarrow f(r)f(r') \in I$$
$$\Rightarrow f(rr') \in I$$
$$\Rightarrow rr' \in f^{-1}(I).$$
2. For any ideal $I$, we have that $0 \in I$. Hence $f^{-1}(0) \subseteq f^{-1}(I)$ and by the definition $\ker(f) = f^{-1}(0)$.

3. By the definition we have $f(f^{-1}(I)) = \{f(x) | x \in f^{-1}(I)\} = \{f(x) | f(x) \in I\}$, which means $f(f^{-1}(I)) = \text{Im}(f) \cap I$.

Since $f$ is onto, we have $f(f^{-1}(I)) = I$.

4. We have already showed that $f^{-1}$ defines a function between the mentioned sets. So it is enough to show that it is injective and surjective.

**Injective**: We have to show that if $f^{-1}(I_1) = f^{-1}(I_2)$, then $I_1 = I_2$.

Assume to the contrary that $I_1 \neq I_2$. So either there is $x \in I_1 \setminus I_2$ or $x \in I_2 \setminus I_1$. Without loss of generality, let us assume that the former holds. Since $f$ is onto, there is $y \in R$ such that $f(y) = x$. But this means that $y \in f^{-1}(I_1) \setminus f^{-1}(I_2)$, which contradicts the assumption that $f^{-1}(I_1) = f^{-1}(I_2)$.

**Surjective**: Let $J$ be an ideal of $R$ which contains $\ker(f)$. Then we claim that (1) $f(J)$ is an ideal in $S$ and (2) $J = f^{-1}(f(J))$. It is clear that (1) and (2) finish the proof of Lemma.

(1) You can prove it using the fact that $f$ is onto.

(2) By the definition, you can check that $J \subseteq f^{-1}(f(J))$. Now we prove that $f^{-1}(f(J)) \subseteq J$.

$x \in f^{-1}(f(J))$ \implies f(x) \in f(J)$ \implies $\exists y \in J$, $f(x) = f(y)$ \implies $\exists y \in J$, $f(x - y) = 0$ \implies $\exists y \in J$, $x - y \in \ker(f) \subseteq J$ \implies $x \in J$. 

\[\square\]

**Corollary 5.** Any homomorphic image of a PIR is a PIR.

**Lemma 6.** $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if $n$ is either 0 or prime.

**Proof.** If $n$ is a composite number, then there are $1 < a, b < n$ such that $ab = n$. Hence $a + n\mathbb{Z}$ and $b + n\mathbb{Z}$ are non-zero and their product is zero. So $\mathbb{Z}/n\mathbb{Z}$ has zero-divisors.

If $p$ is prime, then $p|ab$ if and only if either $p|a$ or $p|b$. Hence $\mathbb{Z}/p\mathbb{Z}$ is a unital (non-trivial) commutative ring without zero-divisors.

If $n = 1$, then $\mathbb{Z}/n\mathbb{Z}$ is the trivial ring which is not an integral domain (by the definition).

**Corollary 7.** If $n$ is a composite integer, then $\mathbb{Z}/n\mathbb{Z}$ is PIR but not PID.

**Example 8.** $\mathbb{Z} \oplus \mathbb{Z}$ is a PIR which is not PID. (I leave the proof of it as an exercise.)

There are several rings which are NOT PIR.

**Example 9.** $\bigoplus_{i=1}^{\infty} \mathbb{Z}$ is an ideal of $\prod_{i=1}^{\infty} \mathbb{Z}$ and it is not a principal ideal. (I leave the proof of this as an exercise.)

**Lemma 10.** The ideal $I$ generated by 2, $x$ in $\mathbb{Z}[x]$ is NOT a principal ideal. In particular, $\mathbb{Z}[x]$ is an integral domain which is not a PID.

**Proof.** Assume to the contrary that there is $p(x) \in \mathbb{Z}[x]$ such that $(2, x) = (p(x))$.

So there is $q(x) \in \mathbb{Z}[x]$ such that $2 = p(x)q(x)$. Since $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$, we have that $p(x) = a \in \mathbb{Z}$ and moreover $a|2$. So $p(x) = \pm 1$ or $p(x) = \pm 2$. However the ideal generated by $\pm 1$ is the whole ring $\mathbb{Z}[x]$. Thus $p(x) = \pm 2$. But this is not possible, either, as $x \not\in \langle \pm 2 \rangle$. (If $x \in \langle \pm 2 \rangle$, then there is a
polynomial \( q(x) \in \mathbb{Z}[x] \), such that \( x = 2q(x) \). But it is not possible as all the coefficients of \( 2q(x) \) are even and \( x \) has an odd coefficient.

Example 11. \( \mathbb{Z}[\sqrt{6}] \) is an integral domain and not a PID. (I leave the proof of this as an exercise.) Let me just remark that later we will see that any PID has unique factorization property. But here \( 6 = 2 \times 3 = \sqrt{6} \times \sqrt{6} \).