CLASS 3, FRIDAY FEBRUARY 9TH: IDEALS & ISOMORPHISM THEOREMS

Last time, we developed the notion of an ideal $I \subseteq R$. Now, we exploit this idea further.

Theorem 0.1 (First Isomorphism Theorem for Rings)**.**
Let $\varphi : R \to S$ be a homomorphism of rings, and let $I = \ker(\varphi)$. Then $\varphi = \varphi' \circ q$, where $q : R \to R/I$ and $\varphi' : R/I \to S : r + I \mapsto \varphi(r)$.

In addition, any ideal is the kernel of the morphism q described above. Thus there exists a bijection

$$\{\textit{kernels of homomorphisms from } R\} \leftrightarrow \{\textit{Ideals of } R\}$$

We have essentially proved this as a remark at the end of last class.

Example 0.2. Let's try to think about ideals of $\mathbb{Z}[x]$ (there are many). Here is one example: Let $\varphi : \mathbb{Z}[x] \to \mathbb{C}$ by taking $\mathbb{Z}$ to itself and $x \mapsto i$. This is a valid ring homomorphism, defining $\varphi(x^n) = \varphi(x)^n = i^n$. What is the kernel? One can check that $x^2 + 1$ is a generator of the kernel. So there is a natural ideal $\langle x^2 + 1\rangle$.

Another example are the projections $\mathbb{Z}[x] \to \mathbb{Z}$, $\mathbb{Z}[x] \to \mathbb{Z}/n\mathbb{Z}$, and $\mathbb{Z}[x] \to \mathbb{Z}/n\mathbb{Z}[x]$. In each case, I am either quotienting out $\mathbb{Z}$ by a number or setting x to be 0. These yield the ideals $\langle x\rangle$, $\langle n, x\rangle$, $\langle n\rangle$ respectively.

We can expand to give the complete list of isomorphism theorems for rings:

Theorem 0.3 (2nd - 4th Isomorphism Theorems for Rings)**.**

2) *Let A be a subring of R, and I be an ideal of R. Then $A + I$ is a subring of R, and $A \cap I$ is an ideal of A. Furthermore,*
$$(A + I)/I \cong A/(A \cap I).$$
3) *Let $I \subset J$ be ideals of a ring A. Then J/I is an ideal of A/I, and*
$$A/J \cong (A/I)/(J/I)$$
4) *Let I be an ideal of R. Then there is a inclusion preserving bijection*
$$\{\textit{Subrings } A \textit{ containing } I\} \leftrightarrow \{\textit{Subrings of } A/I\}$$
Furthermore, A is an ideal of R if and only if A/I is an ideal of R/I.

Proof. 2) $A + I$ is a subring of R, since it is closed under addition, and
$$(a + i)(a' + i') = aa' + ai' + ia' + ii'$$
$aa' \in A$, and $ai', ia', ii' \in I$.

Similarly, $I \cap A$ is an ideal of A, since $a \cdot i \subset I$ in R, and thus if $i \in A \cap I$, then $a \cdot i \in A \cap I$.

Finally, consider the composition $A \to A + I \to A + I/I$, sending a to $a + I$. This is a surjective map as any $a + i + I$ is realized as the image of a. It only goes to compute the kernel. An element $a \in A$ is sent to $0 + I$ if and only if $a \in I$. Thus $a \in A \cap I$. Therefore the kernel is exactly $A \cap I$, which implies that $A/A \cap I \cong (A + I)/I$.

3) The fact that J/I is an ideal is left as an exercise. Consider the quotient map $R/I \to R/J : r + I \mapsto r + J$. This is surjective since $J \supset I$. The kernel is $r + I \subseteq J$, which since $I \subseteq J$, implies $r \in J$ by contraposition. Therefore the kernel is exactly J/I.
4) If I is a subset of A, then $A/I \subseteq R/I$ is a subring. In the opposing direction, if B is a subring of R/I, then we can consider $q^{-1}(B) \subseteq R$. This is a subring by the same algebraic tricks of the second isomorphism, and contains I since $I = q^{-1}(0) \subseteq q^{-1}(B)$. The statement about ideals is a fun exercise.

$\square$

Example 0.4. Consider the ring $R = \mathbb{Z}/n\mathbb{Z}$ for some positive integer $n > 1$. Let's try to find the ideals of R.

By Isomorphism Theorem 4, we know that $J/n\mathbb{Z} \subseteq \mathbb{Z}/n\mathbb{Z}$ is an ideal if and only if $J \subset \mathbb{Z}$ is an ideal containing $n\mathbb{Z}$.

What are the ideals containing $n\mathbb{Z}$ in $\mathbb{Z}$? They are simply $m\mathbb{Z}$ where $m|n$. So if n has a prime factorization of

$$n = p_1^{k_1} \cdots p_l^{k_l}$$

any m of the form $p_1^{k_1'} \cdots p_l^{k_l'}$ where at $k_j' \leq k_j$ works. This completely classifies all ideals of $\mathbb{Z}/n\mathbb{Z}$.

Finally, here are a few operations one can perform on ideals:

- (The Sum) For two ideals I, J, we can form the ideal $I + J$ to be
$$I + J = \{i + j \;:\; i \in I,\; j \in J\}$$
Note that since $0 \in I, J$, we have that $I, J \subseteq I + J$.
- (The Product) We can form the product of two ideals as follows:
$$I \cdot J = \{\sum_{k=0}^{l} i_k \cdot j_k \;:\; i \in I,\; j \in J\}$$
Note in particular that it is NOT strictly the product of two such elements, to be seen momentarily.
- (The Intersection) We can intersect two ideals set theoretically to produce an ideal $I \cap J$ contained in both (**check!**). It contains the product (sometimes properly).
- (The Power) We can iterate the product as above to produce $I^n = I \overset{n-times}{\cdots} I$.

Here are two quick examples to demonstrate some points for these operations:

Example 0.5 (Intersection vs Product)**.** $I \cdot J \subset I \cap J$, because any one of the elements must be in both I and J by strong closure under multiplication. However they are not always the same. For example, let $R = \mathbb{Z}$, and $I = \langle 6 \rangle$ and $J = \langle 10 \rangle$. Their intersection is seen to be $\langle 30 \rangle$, but their product is $\langle 60 \rangle$.

Example 0.6 (Fake product is NOT an ideal)**.** Suppose we defined $I \cdot J$ to be the set of elements of the form $i \cdot j$. Let $R = K[x, y, z, w]$, and consider the ideals $I = \langle x, y \rangle$ and $J = \langle z, w \rangle$. Then elements of the fake product would be xz, xw, yz, yw and any products of various elements with these elements. An ideal needs to be closed under addition, so $xz + yw \in I \cdot J$. However, this is not the case as one can check $xz + yw$ is irreducible (usually called the quadric surface), and thus not a product of elements of I and J.