CLASS 2, WEDNESDAY FEBRUARY 7TH: HOMOMORPHISMS & IDEALS

Recall we left off with the following result:

Corollary 0.1. *Any finite integral domain R is a field.*

We can show existence of inverses using the previous result. The fact that R is commutative is a result of Wedderburn to be shown later.

As with every realm of math, the objects of study are very important, but often times the maps are more important even themselves encoding the information of the ring itself! This brings about the notion of a homomorphism:

Definition 0.2. Let R and S be rings. A map $\varphi : R \to S$ is said to be a **ring homomorphism** if the following criteria are met:

For any $r, r' \in R$, $\varphi(r + r') = \varphi(r) + \varphi(r')$ and $\varphi(rr') = \varphi(r)\varphi(r')$.

The collection (group) of all homomorphisms from R to S is denoted by $\mathrm{Hom}(R, S)$.

This is a very reasonable definition, as it makes addition and multiplication in R compatible with that in S.

Definition 0.3. The **kernel** of φ, denoted $\ker(\varphi)$ is the set

$$\ker(\varphi) = \{r \in R \mid \varphi(r) = 0\} \subseteq R$$

The **image** of φ, denoted $\mathrm{im}(\varphi)$, is the set

$$\mathrm{im}(\varphi) = \{s \in S \mid \exists r \in R \ s.t.\ \varphi(r) = s\} \subseteq S$$

Both are subrings of their respective rings (**proof?**). In the case where $\ker(\varphi) = 0$ and $\mathrm{im}(\varphi) = S$, we say that φ is an **isomorphism**.

As a quick exercise, check that an isomorphism has a ring homomorphism $\psi : S \to R$ which is an inverse to φ.

Example 0.4.
- What is $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z})$?
- What about $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$?
- Consider $\varphi_\alpha : \mathbb{Q}[x] \to \mathbb{Q}$ defined by sending x to $\alpha \in \mathbb{Q}$.

Proposition 0.5. *Any homomorphism $\varphi : R \to S$ can be factored into a surjection $R \to R'$, followed by an injection $R' \to S$.*

This requires us to introduce the notion of **fibers**: Since $\varphi : R \to S$ is in particular a morphism of abelian groups (under addition), we can realize the kernel of this morphism as an abelian group I. We can thus form a ring of cosets

$$R/I = \{r + I \ : \ r \in R\}$$

This is most often called the **quotient ring** of R by I, and it has well defined $+$ and $\cdot$ inhereted from R itself.

The fibers of φ are $r+I$ for a choice of r, as you want to think of them as the preimage of some element of S.

$R' = R/I$ is the desired ring. One can check the existence of homomorphisms as in Proposition 0.5.

Next up, we study **Ideals**. They are often used to describe the structure of R in commutative algebra and algebraic geometry.

Definition 0.6. A subset $I \subseteq R$ is called a **left ideal** if

1º $(I, +)$ is a closed subgroup of R.
2º I is strongly closed under multiplication: For any element $r \in R$ and $\alpha \in I$, we have that $r \cdot i \in I$.

I is called a **right ideal** if the same is true, but for $\alpha \cdot r$. Finally, if I is both a left and right ideal, then I is called a **2-sided ideal**, or simply an **ideal**.

When we eventually specialize our attention to commutative rings, we will only say ideal as all of the above notions coincide.

Example 0.7.
- $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.
- $xK[x]$ is an ideal of $K[x]$.
- Elements divisible by x or y form an ideal of $K[x, y]$.

There is a theme here of divisibility: We can think of all of these ideals as being **generated** by a given element (the smallest ideal containing a given element). In this case, we often refer to them as $\langle n\rangle$, $\langle x\rangle$, or $\langle x, y\rangle$ in the previous cases.

Proposition 0.8. *Let R be a ring and I a (2-sided) ideal. Then R/I as defined above exists and is well defined. In fact, any subring I with this property is necessarily an ideal!*

Proof. R/I clearly makes sense with respect to addition. For multiplication, note that

$$(r + I) \cdot (s + I) = r \cdot s + r \cdot I + I \cdot s + I \cdot I = r \cdot s + I$$

since $r \cdot I, I \cdot s, I \cdot I \subseteq I$.

Now suppose I is an additive subgroup. Then

$$\begin{aligned} r + I &= (r + I)(1 + I) = r + r \cdot I + I + I^2 \\ &= (r + I)(1 + I) = r + I + I \cdot r + I^2 \end{aligned}$$

This implies $r \cdot I, I \cdot r \subseteq I$, as desired. $\square$

As an immediate consequence, the kernel of any homomorphism is a 2-sided ideal! This leads us to our first isomorphism theorem for rings... Next Time!