NOVEMBER 9 NOTES

1. 7.3: Ring Homomorphisms and Quotient Rings

Reminders from last time:

Definition 1.1. Let R and S be rings.

(1) A **ring homomorphism** is a map $\phi : R \to S$ such that, for all $a, b \in R$, $\phi(a+b) = \phi(a)+\phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$.
(2) The **kernel** of ϕ is
$$\ker \phi = \{r \in R \mid \phi(r) = 0\}.$$
(3) An **isomorphism** is a bijective homomorphism.

Proposition 1.2. *Let R and S be rings and $\phi : R \to S$ a homomorphism. Then,*

(1) The image of ϕ is a subring of R, and
(2) The kernel of ϕ is a subring of R. Furthermore, if $a \in \ker \phi$ and $r \in R$ is any element, then $ar \in \ker \phi$.

This last comment on the kernel is an example of something called an *ideal*.

Definition 1.3. Let R be a ring. Let I be a subset of R and let $r \in R$ be an element. Let $rI = \{ra \mid a \in I\}$ and $Ir = \{ar \mid a \in I\}$.

(1) I is called a **left ideal** of R if I is a subring of R and I is closed under left multiplication by elements in R, i.e. $rI \subset I$ for all $r \in R$.
(2) I is called a **right ideal** if I is a subring and I is closed under right multiplication: $Ir \subset I$ for all $r \in R$.
(3) I is called an **ideal** (or sometimes, a **two-sided ideal**) if it is both a left ideal and a right ideal.

Example 1.4. The subring $\mathbb{Z} \subset \mathbb{Q}$ is **not** an ideal. If $r = 1/2 \in \mathbb{Q}$, then $r\mathbb{Z} \not\subset \mathbb{Z}$.

Example 1.5. Let I be an ideal of $\mathbb{Z}$. Then, I must be a subgroup of $\mathbb{Z}$, and the only subgroups of $\mathbb{Z}$ are $\langle n \rangle = \{na \mid a \in \mathbb{Z}\}$ for some $n \in \mathbb{Z}$. These are just the sets of multiples of n, so are indeed ideals: sums and products of multiples of n are again multiples of n, and any multiple of a multiple of n is again a multiple of n. We will write this ideal as (n).

The last part of the previous proposition proves that the kernel of any ring homomorphism is also an ideal.

We can use ideals to define **quotient groups**.

Definition 1.6. Let R be a ring and let I be an ideal of R. Then, the quotient group R/I is a ring with binary operations
$$(r + I) + (s + I) = (r + s) + I \quad \text{(this is just the quotient group structure)}$$
and
$$(r + I) \times (s + I) = (rs) + I.$$
This ring is called the **quotient ring** of R by I.

Just as we had for groups, we have the same properties of quotient rings as we did of quotient groups. Their proofs are almost identical to the proofs of the corresponding statements for groups.

Theorem 1.7. *(1) (The First Isomorphism Theorem.) If $\phi : R \to S$ is a ring homomorphism, then the kernel of ϕ is an ideal of R and $R/\ker\phi \cong \phi(R)$, where the image $\phi(R)$ is a subring of S.*

(2) If I is any ideal of R, then the map $\pi : R \to R/I$ given by $\pi(r) = r + I$ is a surjective ring homomorphism with kernel I. Every ideal is the kernel of a ring homomorphism and vice versa.

(3) (The Second Isomorphism Theorem.) Let A be a subring and B an ideal of R. Then, $A + B = \{a + b \mid a \in A, b \in B\}$ is a subring of R and $A \cap B$ is an ideal of A such that $(A + B)/A \cong A/(A \cap B)$.

(4) (The Third Isomorphism Theorem.) Let I and J be ideals of R with $I \subset J$. Then, J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.

(5) The subrings (resp. ideals) of R/I are precisely the subrings (resp. ideals) of R containing I.

Continuing the example above:

Example 1.8. For any ring R, $R[x]/\{p(x) \mid p(0) = 0\} \cong R$. We saw above that $ev_0 : R[x] \to R$ is a ring homomorphism with kernel $\{p(x) \mid p(0) = 0\}$, and this is surjective because for any $r \in R$, $ev_0(x + r) = r$, so the First Isomorphism Theorem implies that $R[x]/\{p(x) \mid p(0) = 0\} \cong R$.

Some final ideal definitions:

Definition 1.9. Let I and J be ideals of R.

(1) The **sum** of I and J is $I + J = \{a + b \mid a \in I, b \in J\}$.

(2) The **product** of I and J is $IJ = \{a_1b_1 + \cdots + a_nb_n \mid n \in \mathbb{Z}, a_i \in I, b_i \in J\}$ (all finite sums of products of elements in I and J).

(3) For $n \in \mathbb{Z}$, the nth **power** of I is I^n, the set of all finite sums of elements $a_1 \dots a_n$ with $a_i \in I$.

2. 7.4: Properties of Ideals

Now, we define several other important types of ideals. Let R be a ring with identity $1 \neq 0$.

Notation. Let A and B be subsets of R. Then, AB is the set of all finite sums of elements of the form ab where $a \in A$ and $b \in B$, i.e. $AB = \{a_1b_1 + \cdots + a_nb_n \mid n \in \mathbb{Z}, a_i \in A, b_i \in B\}$.

Definition 2.1. Let A be any subset of R.

(1) The **ideal generated by** A is (A), the smallest ideal of R containing A. (One can write $(A) = \cap_{A\subset I,\quad I \text{ ideal}} I$.)

(2) An ideal generated by a single element is called a **principal ideal**.

(3) An ideal generated by a finite set is called a **finitely generated ideal**.

In general, it is difficult to write the ideal generated by an arbitrary set, but we can write the ideal generated by a single element:

If R is commutative and $a \in R$, then $(a) = \{ra \mid r \in R\}$.

Example 2.2. By the earlier example, every ideal of $\mathbb{Z}$ is principal, because every ideal of $\mathbb{Z}$ is of the form (n) for some $n \in \mathbb{Z}$.

Suppose $n, m \in \mathbb{Z}$ are two nonzero integers. Then, $(n, m) = (d)$ where $d = \gcd(n, m)$. Clearly, $(n, m) \subset (d)$ because any finite sum of multiples of n and m is a multiple of d. Also, $d \in (n, m)$ because there exist integers a, b such that $d = an + bm$, so $(d) \subset (n, m)$. Therefore, $(n, m) = (d)$.

Proposition 2.3. *Let I be an ideal of R. Then:*

(1) $I = R$ if and only if I contains a unit.

(2) Assume R is commutative. Then, R is a field if and only if its only ideals are (0) and R.

Proof. For (1), if $I = R$, then $1 \in I$ so I contains a unit. Conversely, suppose $u \in I$ is a unit. Then, there is some $v \in R$ such that $uv = 1$, but I is an ideal, so $u \in I$ implies $1 = uv \in I$. As any $r \in R$ can be written as $r1$, $1 \in I$ implies $r = r1 \in I$ so $R \subset I$ and therefore $R = I$.

For (2), recall that R is a field if and only if every nonzero element is a unit. Therefore, if I is a nonzero ideal, then I contains a unit, so $I = R$ by (1). Conversely, suppose R and (0) are the only ideals of R. Let $u \in R$ be any nonzero element. Then, (u) is a nonzero ideal, so $(u) = R$, so $1 \in (u)$ so there exists some $v \in R$ such that $1 = vu$ and hence u is a unit. □

Corollary 2.4. If R is a field, then any nonzero homomorphism $\phi : R \to S$ is injective.

Proof. The kernel of ϕ must be an ideal of R, but by the previous proposition, $\ker \phi = (0)$ (it cannot be R as ϕ is not zero), so ϕ is injective. □

One important class of ideal is the notion of 'maximal' ideal.

Definition 2.5. An ideal M in a ring R is **maximal** if $M \neq R$ and the only ideals containing M are M and R.

Another type of ideal is a prime ideal.

Definition 2.6. Let R be a commutative ring. A **prime ideal** is a proper ideal P of R such that, for $a, b \in P$, $ab \in P$ implies a or $b \in P$.