Abstract Algebra
Lecture 12
Wednesday, 10/13/2010

1 Ideals

1.1 Quotient Rings

Recall: If I is an ideal of a ring R, then $R/I = \{r + I \mid r \in R\}$ is a ring with operations

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

$$(r + I)(s + I) = (rs) + I$$

Proof: Last time, we proved that, when I is an ideal, these operations are well-defined. We still need to check our ring axioms, however. This is pretty trivial. Left as an exercise for the reader. ∎

Remark: We sometimes talk about **left ideals** or **right ideals**. A left ideal is a subring that only absorbs multiplication on the left ($ri \in I$), and a right ideal is the opposite ($ir \in I$). If we mod out by a one-sided ideal, the result will not be a ring.

1.2 Ring Isomorphism Theorems

Theorem: The First Isomorphism Theorem:
If $f : R \to S$ is a homomorphism, then $R/\ker(f) \cong \mathrm{Im}(f)$ as rings.

Proof: We already know that this holds for the additive group structure. We even have an explicit isomorphism already. We just need to check that it holds for the multiplicative structure. Our isomorphism is: if $I = \ker(f)$, then $\varphi : r + I \mapsto f(r)$. Check $\varphi((r + I)(s + I)) = \varphi(rs + I) = f(rs) = f(r)f(s) = \varphi(r + I)\varphi(s + I)$ as desired. ∎

Theorem: The Second Isomorphism Theorem:
Let I be an ideal of R, and let A be any subring of R. Then $A + I = \{a + i \mid a \in A, i \in I\}$ is a subring of R. Moreover, I is an ideal of $A + I$, and $A \cap I$ is an ideal of A. And

$$(A + I)/I \cong A/(A \cap I).$$

Proof: Again, we have already shown this to be true for the additive group structure. We skip showing the ideals, as that is routine. Our isomorphism as groups is $f : (A + I)/I \to A/(A \cap I)$ given by $(a + i) + I = a + I \to a + (A \cap I)$. Check that this respects multiplication - left as an exercise for the reader. ∎

Theorem: The Third Isomorphism Theorem:
If I, J are ideals of R, and $I \subseteq J$, then

$$(R/I)/(J/I) \cong R/J.$$

Implicit in this is that I is an ideal of J, and J/I is an ideal of R/I.

Proof: Again, this holds for the additive group structure. Our isomorphism is $(r + I) + J/I \mapsto r + J$. Again, simply check that this respects multiplication. ∎

Theorem: The "Fourth" Isomorphism Theorem:
If I is an ideal of R, then there is a bijection

$$\{\text{subrings of } R \text{ that contain } I\} \cong \{\text{subrings of } R/I\}.$$

This bijection respects inclusion and "idealness."

Proof: What is this bijection?

$$I \subseteq A \mapsto A/I \subseteq R/I$$

This proof is part of our homework for this weekend. (The preimage of an ideal is an ideal: given $B \subseteq R/I$, its preimage is $f^{-1}(B)$ where $f : R \to R/I$ – this is what we will actually prove.) ∎

1.3 Combinations of Ideals

Theorem: If I and J are ideals of R, then the following are also ideals:

- $I + J = \{i + j \mid i \in I, j \in J\}$
- $I \cap J$
- $IJ = \{i_1 j_1 + i_2 j_2 + \cdots + i_n j_n \mid i \in I, j \in J\} \subseteq I \cap J$

Proof: Check IJ, for example. First, check that it is a subring. We can see $i_1 j_1 + \cdots + i_n j_n - (i'_1 j'_1 + \cdots + i'_m j'_m) \in IJ$. It also absorbs multiplication: $r(i_1 j_1 + \cdots + i_n j_n) = r i_1 j_1 + \cdots + r i_n j_n = i'_1 j_1 + \cdots + i'_n j_n \in IJ$. ∎

Ex: Let $R = \mathbb{Z}$, $I = 2\mathbb{Z}$, $I = 3\mathbb{Z}$. Then $I + J = \mathbb{Z}$, since $I + J$ includes 1, so $I + J$ must be all of $\mathbb{Z}$. $IJ = 6\mathbb{Z}$. $I \cap J = \mathbb{Z}$ as well. Let $K = 4\mathbb{Z}$. Then $IK = 8\mathbb{Z}$, $I \cap K = 4\mathbb{Z}$, $I + K = 2\mathbb{Z}$. These ideals in Z are each generated by a single element. These are called principal ideals.

1.4 Principal Ideals

Defn: The ideal generated by a single element $a \in R$ is the smallest ideal containing a. We call this the **principal ideal** by a and denote it (a).

For a general ring, $\{a\}$ will probably not be an ideal. We need to have all multiples of a. Since this is a general ring, we need to worry about both left and right multiplication. So how about $\{ras \mid r, s \in R\}$? This is still not quite enough - it generally won't be closed under addition. So the true ideal is

$$(a) = \{r_1as_1 + \cdots + r_nas_n \mid r_i, s_i \in R\}$$

. We can show that every ideal that contains a has this as a subset, thus this is the minimum ideal containing a, thus it is the principal ideal.

Theorem: In a commutative ring R, $(a) = \{ra \mid r \in R\}$.

Proof: We know that $(a) = \{r_1as_1 + \cdots + r_nas_n \mid r_i, s_i \in R\} = \{r_1s_1a + \cdots + r_ns_na\} = \{(r_1s_1 + \cdots + r_ns_n)a\} = \{ra\}$. ∎

Ex: Note that $6 \in 2\mathbb{Z}$, $6 \in 3\mathbb{Z}$, but $6 \notin p\mathbb{Z}$ for any other prime p. So principal rings are telling us something about divisibility in our ring.

Theorem: $b \in (a) \iff a|b$.

Defn: We can also look at ideals generated by more than one element. If A is any subset of R, then

$$(A) = \{r_1a_1s_1 + \cdots + r_na_ns_1 \mid r_i, s_i \in R, a_i \in A\}.$$