

Handout 12: Congruence and quotient rings

As we've already seen, ideals are to rings much as normal subgroups are to groups. It shouldn't be overly surprising, therefore, that we can "divide" a ring R by one of its ideals, I , in exactly the same way we'd "divide" a group G by one of its normal subgroups, N . Let's make this more precise.

Definition. Let R be a ring and let I be an ideal in R . We say that a and b are _____ mod I , and we write _____, if and only if $a - b \in I$.

Proposition (Lemma 3.104). \equiv_I is an _____ relation on R .

Proof. Three things to check; go ahead and do it!

The equivalence (or *congruence*) class of $a \in R$ modulo I is denoted $[a]_I$, or simply $[a]$, and the set of all such classes is

$$R/I = \{[a]_I \mid a \in R\}.$$

Wouldn't it be lovely if we could make this object, the *quotient* of R modulo I , into a ring?

This would require that we can come up with *well-defined* operations, $+$ and \cdot , on R/I . How could we define such operations?

Okay, then, why are these operations well-defined? (**Note:** this is the content of Lemma 3.105 of your text.)

Note. Recall that your textbook simply assumes that all rings are commutative (at least for now), whereas we have not made such an assumption.

Theorem (3.106). If R is a ring with ideal I , then the set R/I becomes a ring with the operations defined above, and is called the _____ ring of R by I . If R is commutative, then so is R/I .

Proof. This is really just a tedious step-by-step verification of the axioms. Let's just prove one of the more challenging ones (the remaining ones are proven on page 292 of your textbook)...maybe we can check distributivity of products over sums:

See how easy?

Proposition/Definition. Let R be a ring and let I be an ideal in R . If $a \in R$, then the set

$$a + I = \{a + i \mid i \in I\},$$

called the _____ of a modulo I , satisfies $[a]_I = a + I$.

Proof. This is nothing too difficult:

Examples. For each example given below, (a) describe the structure of the given ideal I , and (b) describe the structure of R/I .

1. $R = \mathbb{Z}$ and $I = (n)$ for some fixed $n \in \mathbb{Z}$

2. $R = \mathbb{Z}_n$, and $I = (k)$ for some fixed k , $0 \leq k \leq n - 1$

3. $R = \mathcal{P}(X)$ for some set X , and $I = (A)$ for some $A \subseteq X$

Our next step is discuss the structure of R/I more carefully, and to relate its structure to the appropriate ring homomorphism. (Does someone sense a big theorem coming on?)

Homework. Here are a few homework problems; a couple of committee problems are marked with “(CP).”

1. **(CP)** Do exercise 3.93 on page 303. (*Hint:* define the appropriate isomorphism and prove that it really is an isomorphism. It might help to think of the the division process in the following light: when you form the quotient R/I , you’re essentially “collapsing” all of I to 0.)
2. Let R be a ring. Describe the quotient $R[x]/(x^2)$ as well as you can, proving any claims that make. (*Hint:* an optimal solution would define a ring to which $R[x]/(x^2)$ is isomorphic, proving the isomorphism.)
3. **(CP)** Let R be a ring. Fill in the blank, and prove carefully that the resulting claim is true:
 $R/(0) \cong \underline{\hspace{2cm}}$.

Here is a schedule for this homework:

- **Monday, March 2nd.** Committee problems due to committees.
- **Wednesday, March 4th.** Committees present reports to class.
- **Friday, March 6th.** All homework due at 5:00 p.m.