

## Lecture 11 (Ideals and Quotient Rings)

**Definition 11.1 (Congruences)** Let  $R$  be a ring and  $\equiv$  an equivalence relation on  $R$ . Then  $\equiv$  on  $R$  is called a congruence if for all  $x, x', y, y' \in R$ ,  $x \equiv x'$  and  $y \equiv y'$  imply

$$x + y \equiv x' + y' \quad \text{and} \quad xy \equiv x'y'.$$

Equivalently  $\equiv$  is a congruence if  $\bar{x} = \bar{x'}$  and  $\bar{y} = \bar{y'}$  imply

$$x + y \equiv x' + y' \quad \text{and} \quad xy \equiv x'y'.$$

If  $\equiv$  is a congruence then we have well defined addition and multiplication operations on the set  $R/\equiv$  of equivalence classes of  $\equiv$ , inherited from  $R$ :

$$\begin{aligned} \bar{x} + \bar{y} &= \overline{x + y} \\ \overline{xy} &= \overline{xy} \end{aligned}$$

Conversely for these operations to be well defined  $\equiv$  must be a congruence.

**Proposition 11.2** Suppose  $\equiv$  is a congruence on a ring  $R$ .

- (1) The addition and multiplication inherited from  $R$  make  $R/\equiv$  into a ring.
- (2) The canonical map  $R \rightarrow R/\equiv$ , such that  $x \mapsto \bar{x}$  is a surjective ring homomorphism.
- (3) If  $R$  is commutative so is  $R/\equiv$ .

If  $R$  has identity element 1,  $R/\equiv$  has identity element  $\bar{1}$ .

**Proof** Note the canonical map from a set to its equivalence classes under a relation is always surjective, and by the definition of addition and multiplication the canonical map preserves addition and multiplication. So (2) follows as soon as (1) is proved.

Proof of (1). Ring axioms and properties in  $R/\equiv$  are inherited from  $R$ , c.f. Tutorial 2 Question 1.

Elements of  $R/\equiv$  are all of the form  $\bar{x}$  from some  $x \in R$ .

Suppose  $\bar{x}, \bar{y}, \bar{z} \in R/\equiv$ .

Using the fact that the canonical map preserves addition, we deduce the following.

From  $x + (y + z) = (x + y) + z$  in  $R$  follows

$$\begin{aligned}\overline{x + (y + z)} &= \overline{(x + y) + z} \\ \bar{x} + \overline{(y + z)} &= \overline{(x + y)} + \bar{z} \\ \bar{x} + (\bar{y} + \bar{z}) &= (\bar{x} + \bar{y}) + \bar{z}\end{aligned}$$

From  $x + y = y + x$  we deduce

$$\begin{aligned}\overline{x + y} &= \overline{y + x} \\ \bar{x} + \bar{y} &= \bar{y} + \bar{x}\end{aligned}$$

From  $x + 0 = x$  in  $R$  follows  $\bar{x} + \bar{0} = \bar{x}$ . Hence  $\bar{0}$  is a zero for addition in the quotient ring. From  $x + (-x) = 0$  follows  $\bar{x} + \overline{-x} = \bar{0}$ . Hence each element  $\bar{x}$  has negative  $-\bar{x} = \overline{-x}$ . So  $R/\equiv$  is an abelian group under addition.

Multiplication is associative in  $R$  so  $x(yz) = (xy)z$  in  $R$  follows

$$\begin{aligned}\overline{x(yz)} &= \overline{(xy)z} \\ \bar{x}\overline{(yz)} &= \overline{(xy)}\bar{z} \\ \bar{x}(\bar{y}\bar{z}) &= (\bar{x}\bar{y})\bar{z}\end{aligned}$$

using the fact that the  $x \mapsto \bar{x}$  respects multiplication.

Similarly the distributive laws in  $R/\equiv$  are inherited from the distributive laws in  $R$ . So for example from the left distributive law in  $R$ ,  $x(y + z) = xy + xz$  in  $R$  follows

$$\begin{aligned}\bar{x}\overline{(y + z)} &= \overline{xy} + \overline{xz} \\ \bar{x}(\bar{y} + \bar{z}) &= \bar{x}\bar{y} + \bar{x}\bar{z}.\end{aligned}$$

the left distributive law in the quotient ring

Thus all the ring axioms are satisfied.

In the same way from  $R$  commutative follows the quotient ring commutative. Lastly if  $R$  has identity 1, from  $1x = x = x1$  in  $R$  follows  $\bar{1}\bar{x} = \bar{x} = \bar{x}\bar{1}$ . Hence  $\bar{1}$  is an identity for  $R/\equiv$ . From the proof we see  $\bar{0}$  is the zero of the quotient and  $\overline{-x} = -\bar{x}$ .  $\square$

The kernel of the canonical map,

$$\{x \in R \mid \bar{x} = \bar{0}\} = \{x \in R \mid x \equiv 0\}.$$

Kernels of homomorphisms are ideals.

**Corollary** If  $\equiv$  is a congruence on a ring  $R$ ,  $\{x \in R \mid \bar{x}\}$  is an ideal of  $R$ . Further if we put  $I = I(\equiv) = \{x \in R \mid \bar{x}\}$  then

$$x \equiv y \Leftrightarrow \bar{x} = \bar{y} \Leftrightarrow \overline{x - y} = \bar{0} \Leftrightarrow x - y \in I.$$

Conversely every ideal defines a congruence, for which  $I(\equiv) = I$ , viz we define  $x \equiv y \pmod I$ , ( $x$  is congruent to  $y$  modulo  $I$ ), if  $x - y \in I$ .

**Lemma 11.3** Suppose  $I$  is an ideal, then  $x \equiv y$  if  $x - y \in I$  is a congruence on  $R$  and  $\{x \mid x \equiv 0\} = I$ .

**Proof** We first show congruence modulo  $I$  is an equivalence relation. Suppose  $x, y, z \in R$ .

Every ideal contains 0. Hence for  $x \in R$   $x - x \in I$ .

Ideals are closed under taking negatives. So  $x - y \in I \Rightarrow y - x = -(x - y) \in I$ .

From  $x - y \in I$ ,  $y - z \in I$  follows  $x - z = (x - y) + (y - z) \in I$  because ideals are closed under addition.

From the above it follows that congruence modulo  $I$  is an reflexive, symmetric and transitive.

We now show this equivalence relation is a congruence.

Suppose  $x \equiv x'$  and  $y \equiv y'$  modulo an ideal  $I$ . So  $(x - x'), (y - y') \in I$ .

By closure of ideals under addition

$$(x + y) - (x' + y') = (x - x') + (y - y') \in I$$

So  $x + y \equiv x' + y' \pmod I$ .

By closure of ideals in a ring under multiplication on the left and right by elements of the ring we have  $(x - x')y, x'(y - y') \in I$ . So by closure of ideals under addition we deduce

$$xy - x'y' = (x - x')y + x'(y - y') \in I.$$

So  $xy \equiv x'y' \pmod I$ . □

If we start with a ring and form the quotient ring for congruence modulo an ideal  $I$  this usually denoted  $R/I$  and the equivalence class of  $x \in R$   $\bar{x} = \{x + a \mid a \in I\}$  by  $x + I$ .