

## Last lecture

- A **ring homomorphism** is a map  $\varphi : R \rightarrow S$  such that  $\varphi(x + y) = \varphi(x) + \varphi(y)$  and  $\varphi(xy) = \varphi(x)\varphi(y)$ , for all  $x, y \in R$ .
- If  $\varphi : R \rightarrow S$  is a ring homomorphism then  $\text{im } \varphi$  is a subring of  $S$  (Proposition 4.6) and  $\ker \varphi$  is a subring of  $R$  (Proposition 4.7).
- $R[x] = \left\{ \sum_{i \geq 0} f_i x^i : |\{i \geq 0 : f_i \neq 0\}| < \infty \right\}$  is the subring of  $R[[x]]$  of polynomials over  $R$  in the indeterminate  $x$ .
- If  $R$  is a commutative ring then  $\text{eval}_r : R[x] \rightarrow R$  is a ring homomorphism for all  $r \in R$  (Proposition 5.7).

## Quotient rings and ideals

### Question

If  $S$  is a subring of a ring  $R$  can we construct a **quotient ring**  $R/S$ ?

For any subring  $S$  of  $R$  the quotient  $R/S = \{r + S : r \in R\}$  inherits a natural addition from  $R$ :  $(r + S) + (r' + S) = (r + r') + S$ .

**Reason**  $(R, +)$  is an **abelian group** so  $S$  is a normal subgroup.

For  $R/S$  to inherit a multiplication as well we need  $S$  be well behaved with respect to multiplication.

### Definition 6.1

An **ideal** of  $R$  is a subring  $I$  such that  $ra, ar \in I$ , for all  $r \in R$  and  $a \in I$ .

Strictly speaking, this is a **two-sided ideal** of  $R$ .

A **left ideal** of  $R$  is a subring  $I$  such that  $ra \in I$ , for  $r \in R$  and  $a \in I$ .

A **right ideal** of  $R$  is a subring  $I$  such that  $ar \in I$ , for  $r \in R$  and  $a \in I$ .

An ideal of  $R$  is a subring which is both a left and right ideal.

## Congruences and quotients

### Definition 6.2

A **congruence** on a ring  $R$  is an equivalence relation  $\approx$  on  $R$  such that if  $a \approx a'$  and  $b \approx b'$  then  $a + b \approx a' + b'$  and  $ab \approx a'b'$ .

Suppose that  $\approx$  is a congruence on  $R$ .

Let  $Q = R/\approx = \{\bar{x} : x \in R\}$ . (Recall  $\bar{x} = \{y \in R : y \approx x\}$ )

### Proposition 6.3

Suppose that  $\approx$  is a congruence on  $R$ . Then  $Q = R/\approx$  is a ring with operations  $\bar{x} + \bar{y} = \overline{x + y}$  and  $\bar{x} \cdot \bar{y} = \overline{x \cdot y}$ , for  $\bar{x}, \bar{y} \in Q$ .

**Proof** We must check that  $Q$  is a ring **and** that the operations on  $Q$  are well-defined; that is, that they do not depend on the choice of  $x$  and  $y$ .

Suppose that  $x \approx x'$  and  $y \approx y'$ . Then, by the definition of congruence,  $x + y \approx x' + y'$  and  $xy \approx x'y'$ . That is,  $\overline{x + y} = \overline{x' + y'}$  and  $\overline{xy} = \overline{x'y'}$ . Hence, the operations on  $Q$  are well-defined.

## Congruences and quotients.../2

$(Q, +)$  is an abelian group

$$(1) \bar{x} + (\bar{y} + \bar{z}) = \overline{x + y + z} = \overline{(x + y) + z} \implies \text{associative}$$

$$(2) \bar{x} + \bar{y} = \overline{x + y} = \overline{y + x} = \bar{y} + \bar{x} \implies \text{abelian.}$$

$$(3) \bar{x} + \bar{0} = \overline{x + 0} = \bar{x} \implies \bar{0} \text{ is the zero element}$$

$$(4) \bar{x} + \overline{-x} = \overline{x - x} = \bar{0} \implies \text{we have negatives}$$

$(Q, \cdot)$  is associative

$$\overline{\bar{x}(\bar{y}\bar{z})} = \overline{x(yz)} = \overline{(xy)z} = \overline{(\bar{x}\bar{y})\bar{z}}.$$

The distributive law

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

Similarly,  $\overline{(\bar{x} + \bar{y})\bar{z}} = \overline{xz} + \overline{yz}$ .

Hence,  $Q$  is a ring. □

**Remark** Howlett gives a slicker proof by showing that if  $\varphi : R \rightarrow S$  is a map from a ring  $R$  into a set  $S$  equipped with an addition and a multiplication then  $\text{im } \varphi$  is a ring.

Here we can take  $\varphi$  to be the map  $R \rightarrow S$  given by  $\varphi(x) = \bar{x}$ .

## Congruences and ideals

### Proposition 6.4

Suppose that  $R$  is a ring.

- 1 If  $\approx$  is a congruence on  $R$  then the set  $I = \{r \in R : r \approx 0\}$  is an ideal of  $R$ .
- 2 If  $I$  is an ideal of  $R$  then  $x \approx y$  if  $x - y \in I$  is a congruence on  $R$ .

**Proof** (1) Suppose that  $\approx$  is a congruence on  $R$ .

Then  $I \neq \emptyset$  since  $0 = 0_R \in I$  (as  $0 \approx 0$ ).

Suppose that  $a, b \in I \implies a \approx 0$  and  $b \approx 0$   
 $\implies -b = -b + 0 \approx -b + b = 0$

Then,  $a - b \approx 0 - 0 = 0 \implies a - b \in I$   
and  $ab \approx 0 \cdot 0 = 0 \implies ab \in I$ .

Hence,  $I$  is closed under addition, negatives and multiplication  
 $\implies I$  is a subring.

If  $r \in R$  then  $ra \approx r \cdot 0 = 0$  and  $ar \approx 0 \cdot r = 0 \implies I$  is an ideal.

## Congruences and ideals.../2

(2) Suppose that  $I$  is an ideal of  $R$  and define  $x \approx y$  if  $x - y \in I$ .

$\approx$  is an equivalence relation

(Reflexive)  $x \approx x$  since  $x - x = 0 \in I$

(Symmetric)  $x \approx y \implies x - y \in I \implies y - x \in I \implies y \approx x$

(Transitive)  $x \approx y$  and  $y \approx z \implies x - z = (x - y) + (y - z) \in I$

Hence,  $\approx$  is an equivalence relation!

$\approx$  is a congruence

Suppose that  $x \approx x'$  and  $y \approx y' \implies x - x', y - y' \in I$

(+) We have,  $(x + y) - (x' + y') = (x - x') + (y - y') \in I$   
 $\implies x + y \approx x' + y'$ .

(.) Write  $x' = x + a$  and  $y' = y + b$  for some  $a, b \in I$ . Then  
 $x'y' = (x + a)(y + b) = xy + xb + ay + ab \approx xy$   
since  $I$  is an ideal (so that  $xb, ay, ab \in I$ ).

Hence,  $\approx$  is a congruence on  $R$ . □

## Quotient rings

By Proposition 6.3 and Proposition 6.4 we can make the following definition

### Definition 6.5

Suppose that  $I$  is an ideal of  $R$ . Then the **quotient ring**  $R/I$  is the set

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

with operations  $(x + I) + (y + I) = (x + y) + I$  and  $(x + I)(y + I) = xy + I$ .

### Proposition 6.6

Suppose that  $I$  is an ideal of  $R$ . Then

- 1 The natural map  $\pi : R \rightarrow R/I; x \mapsto x + I$  is a surjective ring homomorphism with  $\ker \pi = I$ .
- 2 If  $R$  is commutative then  $R/I$  is a commutative ring.
- 3 If  $R$  is a ring with one then  $R/I$  is a ring with one.

## Quotient rings.../

**Proof** (1) If  $x, y \in R$  then

$\pi(x + y) = (x + y) + I = (x + I) + (y + I) = \pi(x) + \pi(y)$  and

$\pi(xy) = xy + I = (x + I)(y + I) = \pi(x)\pi(y)$ .

Hence,  $\pi$  is a homomorphism.

The map is clearly surjective since  $x + I = \pi(x)$ , for  $x \in R$ ,  
and  $x \in \ker \pi \iff \pi(x) = x + I = 0 + I \iff x \in I$ .

(2) If  $R$  is commutative then

$$(x + I)(y + I) = xy + I = yx + I = (y + I)(x + I).$$

(3) If  $R$  has a one  $1_R$  then

$$(1_R + I)(x + I) = x + I = (x + I)(1_R + I). \quad \square$$