Lecture 09: Factor rings

Wednesday, April 18, 2018 4:52 PM

In the previous lecture we were proving:

Theorem. Suppose $I \lhd R$. Then $(R/I, +, \cdot)$ is a ring, where

$(a+I)+(b+I) := (a+b)+I$ and $(a+I)\cdot(b+I) := ab+I$.

We start with recalling the following fact from group theory:

$$\boxed{a+I = b+I \iff a-b \in I.}$$

Pf ($\Rightarrow$) $a \in a+I = b+I \Rightarrow \exists\, c \in I,\ a = b+c$

$\Rightarrow a-b = c \in I.$

($\Leftarrow$) $\forall c \in I,\ a+c = b + \underbrace{\underbrace{(a-b)}_{\text{in } I} + \underbrace{c}_{\text{in } I}}_{\text{in } I} \in b+I \Rightarrow a+I \subseteq b+I$ (1)

Similarly, $\forall c \in I,\ b+c = a - \underbrace{(a-b)+c}_{\text{in } I} \in a+I \Rightarrow b+I \subseteq a+I$ (2)

(1) and (2) imply $a+I = b+I$. ∎

Pf of Theorem + is well-defined. Suppose $a_1+I = a_2+I$ and $b_1+I = b_2+I$. Then

$$\left.\begin{matrix} a_1-a_2 \in I \\ b_1-b_2 \in I \end{matrix}\right\} \Rightarrow (a_1-a_2)+(b_1-b_2) \in I$$

$$\Rightarrow (a_1+b_1)-(a_2+b_2) \in I$$

$$\Rightarrow a_1+b_1+I = a_2+b_2+I$$

• is well-defined.

$$\left.\begin{matrix} a_1+I=a_2+I \\ b_1+I=b_2+I \end{matrix}\right\} \overset{?}{\Longrightarrow} a_1b_1+I=a_2b_2+I$$

$$\Updownarrow \qquad\qquad \Updownarrow$$

$$\begin{matrix} a_1-a_2\in I \\ b_1-b_2\in I \end{matrix} \qquad\qquad a_1b_1-a_2b_2\in I .$$

$$a_1b_1-a_2b_2 = a_1b_1-a_2b_1+a_2b_1-a_2b_2 \qquad \text{(similar to congruence arith.)}$$

$$= (a_1-a_2)b_1 + a_2(b_1-b_2) \in I$$

$a_1-a_2\in I \Rightarrow (a_1-a_2)b_1\in I$

$b_1-b_2\in I \Rightarrow a_2(b_1-b_2)\in I$

Distribution. $\big((a+I)+(b+I)\big)\cdot(c+I) = \big((a+b)+I\big)\cdot(c+I)$

$$= \big((a+b)\cdot c\big)+I$$
$$= (ac+bc)+I$$
$$= \big(ac+I\big)+(bc+I)$$
$$= (a+I)\cdot(c+I)+(b+I)(c+I)$$

As you can see we are doing all the "computations" in R, and "decorate" them with $+I$. So you can see that other properties of operations are inherited from R.

(Exercise finish the above proof.) ∎

Lecture 09: Factor ring and natural homomorphism

Wednesday, April 18, 2018 11:17 AM

Lemma. Suppose $I \lhd R$. Let $p: R \to R/I$, $p(r) := r+I$. Then p is a ring homomorphism and $\ker p = I$, Image of $p = R/I$.

Pf: • $p(a+b) = (a+b)+I = (a+I)+(b+I) = p(a)+p(b)$

• $p(ab) = (ab)+I = (a+I)\cdot(b+I) = p(a)\cdot p(b)$.

So p is a ring homomorphism.

• $r \in \ker p \iff p(r)=0 \iff r+I = 0+I \iff r-0 \in I \iff r \in I$

So $\ker p = I$.

• Image of $p = \{r+I \mid r \in R\} = R/I$. ■

And so ideals are precisely those subsets of R that are kernels of ring homomorphisms.

Theorem (The 1st isomorphism theorem)

Suppose $f: R \to S$ is a ring homomorphism. Then

(1) $\ker f \lhd R$; (2) $\operatorname{Im} f$ is a subring of S;

(3) $\overline{f}: R/\ker f \longrightarrow \operatorname{Im} f$, $\overline{f}(r+\ker f) := f(r)$ is a ring isomorphism.

Pf. (1) we have already proved.

(2) Suppose $y_1, y_2 \in \operatorname{Im} f$. Then $y_1 = f(r_1)$ and $y_2 = f(r_2)$.

And so $y_1 + y_2 = f(r_1) + f(r_2) = f(r_1 + r_2) \in \operatorname{Im} f$,

$y_1 \cdot y_2 = f(r_1) \cdot f(r_2) = f(r_1 \cdot r_2) \in \operatorname{Im} f$.

Therefore by the subring criterion, $\operatorname{Im} f$ is a subring of S.

(3). $\bar{f}$ is well-defined.

$$r_1 + \ker f = r_2 + \ker f \Rightarrow r_1 - r_2 \in \ker f$$
$$\Rightarrow f(r_1 - r_2) = 0 \Rightarrow f(r_1) - f(r_2) = 0$$
$$\Rightarrow f(r_1) = f(r_2).$$

- $\bar{f}$ is injective.

$$\bar{f}(r_1 + \ker f) = \bar{f}(r_2 + \ker f) \Rightarrow f(r_1) = f(r_2)$$
$$\Rightarrow f(r_1) - f(r_2) = 0 \Rightarrow f(r_1 - r_2) = 0$$
$$\Rightarrow r_1 - r_2 \in \ker f \Rightarrow r_1 + \ker f = r_2 + \ker f.$$

- $\bar{f}$ is surjective. $\operatorname{Im} \bar{f} = \operatorname{Im} f$ ✓

- $\bar{f}$ is a ring homomorphism.

$$\bar{f}((a + \ker f) + (b + \ker f)) = \bar{f}((a+b) + \ker f)$$
$$= f(a+b) = f(a) + f(b)$$

$$= \overline{f}(a+\ker f) + \overline{f}(b+\ker f)$$

$$\overline{f}((a+\ker f)(b+\ker f)) = \overline{f}(ab+\ker f)$$

$$= f(ab)$$

$$= f(a)f(b)$$

$$= \overline{f}(a+\ker f)\,\overline{f}(b+\ker f). \blacksquare$$

Ex. $\mathbb{Z}/_{n\mathbb{Z}} \simeq \mathbb{Z}_n$.

Pf. Let $c_n: \mathbb{Z} \to \mathbb{Z}_n$, $c_n(m) :=$ remainder of m divided by n.

c_n is a ring hom. • Argument relies on the following facts:

- Since $c_n(m)$ is the remainder of m divided by n, $m \equiv c_n(m) \pmod n$.
- For $r_1, r_2 \in \mathbb{Z}_n$, $r_1 \equiv r_2 \pmod n \iff r_1 = r_2$.

And so $c_n(a+b) \equiv a+b \equiv c_n(a)+c_n(b)$

$\equiv c_n(a) \oplus c_n(b) \pmod n$, which implies

$c_n(a+b) = c_n(a) \oplus c_n(b)$.

- Similarly $c_n(ab) \equiv ab \equiv c_n(a)\cdot c_n(b)$

$\equiv c_n(a) \odot c_n(b) \pmod n$

And so $c_n(ab) = c_n(a) \odot c_n(b)$.

Lecture 09: Ring of integers modulo n

Wednesday, April 18, 2018 11:45 AM

$\underline{\text{Im } c_n = \mathbb{Z}_n}$. $\forall r \in \mathbb{Z}_n$, $c_n(r) = r$. And so c_n is onto and $\text{Im } c_n = \mathbb{Z}_n$.

$\underline{\ker c_n = n\mathbb{Z}}$. $r \in \ker c_n \iff c_n(r) = 0$

$\iff n \mid r$

$\iff r \in n\mathbb{Z}$.

Therefore by the 1st isomorphism theorem,

$\overline{c_n} : \mathbb{Z}/_{n\mathbb{Z}} \longrightarrow \mathbb{Z}_n$, $\overline{c_n}(r + n\mathbb{Z}) := c_n(r)$ is an isomorphism. ■