

## Homework 2 Solutions.

② Let  $F$  be a field, and let  $\phi: F \rightarrow R$  be a ring hom<sup>m</sup>.

Show:  $\phi$  is either zero or 1-1.

Proof:  $\ker \phi \triangleleft F \Rightarrow \left\{ \begin{array}{l} \ker \phi = (0) \Rightarrow \phi \text{ is 1-1} \\ \text{or } \ker \phi = (1) = F \end{array} \right.$

a field  $F$  only has  
2 ideals:  $(0), (1)$

$\Rightarrow \forall f \in F, \phi(f) = 0$ . I.e.,  $\phi$  is zero.

---

③ Let  $F$  and  $E$  be fields, and let  $\phi: F \rightarrow E$  be a ring hom<sup>m</sup>.

Show:  $\phi$  onto  $\Rightarrow \phi$  is an isom<sup>m</sup>.

Proof: Suppose that  $\phi$  is onto. Show that  $\phi$  is 1-1.

②  $\Rightarrow \phi$  is 1-1 or  $\phi$  is zero. Suppose that  $\phi$  is zero.

$\phi: \text{ring hom}^m \rightarrow \phi(1_F) = 1_E \neq 0_E \Rightarrow \phi \neq 0 \Rightarrow \Leftarrow$ .

Therefore,  $\phi$  is 1-1.

---

⑤ Let  $\phi: \mathbb{Z} \rightarrow \mathbb{Z}$  be a ring hom<sup>m</sup>. Show:  $\forall n \in \mathbb{Z}, \phi(n) = n$ .

Proof:  $\phi: \text{hom}^m \rightarrow \phi(1) = 1 \Rightarrow \forall n \in \mathbb{Z},$

~~Then~~  $\phi(n) = \phi(n \cdot 1) = n \phi(1) = n \cdot 1 = n$ .

(10) Let  $R, S$  be rings, and let  $\phi, \theta: R \rightarrow S$  be ring hom's.

Show:  $\underbrace{\{r \in R : \phi(r) = \theta(r)\}}_{= T}$  is a subring of  $R$ .

Proof: Verify subring axioms:

$$\left. \begin{array}{l} \phi, \theta: \text{hom}^R \Rightarrow \phi(1_R) = 1_S \\ \theta(1_R) = 1_S \end{array} \right\} \Rightarrow 1_R \in T.$$

$$\bullet r_1, r_2 \in T. \text{ Then we have: } \begin{array}{l} \phi(r_1) = \theta(r_1) \\ \phi(r_2) = \theta(r_2) \end{array}$$

$$r_1 \pm r_2 \in T \Leftarrow \begin{cases} \phi(r_1 \pm r_2) = \phi(r_1) \pm \phi(r_2) = \theta(r_1) \pm \theta(r_2) \\ \theta: \text{hom}^R \Rightarrow \theta(r_1 \pm r_2) = \theta(r_1) \pm \theta(r_2) \end{cases}$$

$$\bullet r_1, r_2 \in T. \text{ Then we have: } \begin{array}{l} \phi(r_1) = \theta(r_1) \\ \phi(r_2) = \theta(r_2) \end{array}$$

$$r_1 r_2 \in T \Leftarrow \begin{cases} \phi(r_1 r_2) = \phi(r_1) \phi(r_2) = \theta(r_1) \theta(r_2) = \theta(r_1 r_2) \\ \phi: \text{hom}^R \Rightarrow \phi(r_1 r_2) = \phi(r_1) \phi(r_2) \\ \theta: \text{hom}^R \Rightarrow \theta(r_1 r_2) = \theta(r_1) \theta(r_2) \end{cases}$$

It follows that  $T$  is a subring of  $R$ .

(11) Let  $R_1, R_2 \neq 0$  be rings. Show that  $R_1 \oplus R_2$  is not an integral domain.

Proof:  $\underbrace{(1_{R_1}, 0_{R_2})}_{\neq 0_R \text{ in } R} \cdot \underbrace{(0_{R_1}, 1_{R_2})}_{\neq 0_R \text{ in } R} = (0_{R_1}, 0_{R_2}) = 0_R.$

(13) Find all ring hom<sup>s</sup>:  $\phi: \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z}$ .

Solution: Observe that  $\mathbb{Z} \oplus \mathbb{Z} = \langle (1,0), (0,1) \rangle$ .

Suppose that  $\phi((1,0)) = m$   
 $\phi((0,1)) = n$  }  $\in \mathbb{Z}$ . We must have:

$$\phi(0_{\mathbb{Z} \oplus \mathbb{Z}}) = \phi((0,0)) = \phi((1,0)(0,1)) = \phi((1,0))\phi((0,1)) = mn = 0$$

$$\phi(1_{\mathbb{Z} \oplus \mathbb{Z}}) = \phi((1,1)) = \phi((1,0) + (0,1)) = \phi((1,0)) + \phi((0,1)) = m+n = 1.$$

Hence we must have: <sup>①</sup>  $m=1, n=0$ :  $\phi: \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z}$   
 $(m,n) \mapsto m$ .

or <sup>②</sup>  $m=0, n=1$ :  $\phi: \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z}$   
 $(m,n) \mapsto n$ .

14) Find all ring hom<sup>s</sup>  $\phi: \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z} \oplus \mathbb{Z}$ .

Solution:  $\mathbb{Z} \oplus \mathbb{Z} = \langle (1,0), (0,1) \rangle$

Suppose that  $\phi((1,0)) = (a_1, b_1)$  and  $\phi((0,1)) = (a_2, b_2) \in \mathbb{Z} \oplus \mathbb{Z}$ . We must have:

$$\phi(0_{\mathbb{Z} \oplus \mathbb{Z}}) = \phi((0,0)) = \phi((1,0)(0,1)) = \phi((1,0))\phi((0,1))$$

$$= (a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2) = (0,0) \Rightarrow \begin{array}{l} a_1 a_2 = 0 \\ b_1 b_2 = 0 \end{array}$$

$$\phi(1_{\mathbb{Z} \oplus \mathbb{Z}}) = \phi((1,1)) = \phi((1,0) + (0,1)) = (a_1, b_1) + (a_2, b_2)$$

$$= (a_1 + a_2, b_1 + b_2) = (1,1) \Rightarrow \begin{array}{l} a_1 + a_2 = 1 \\ b_1 + b_2 = 1 \end{array}$$

Hence, we must have one of the following 4 possibilities:

①  $\phi((1,0)) = (1,1)$ ,  $\phi((0,1)) = (0,0)$ . Then  $\phi: \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z} \oplus \mathbb{Z}$   
 $(m,n) \mapsto (m,m)$

②  $\phi((1,0)) = (1,0)$ ,  $\phi((0,1)) = (0,1)$ . Then  $\phi: \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z} \oplus \mathbb{Z}$   
 $(m,n) \mapsto (m,n)$ .

③  $\phi((1,0)) = (0,1)$ ,  $\phi((0,1)) = (1,0)$ . Then  $\phi: \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z} \oplus \mathbb{Z}$   
 $(m,n) \mapsto (n,m)$

④  $\phi((1,0)) = (0,0)$ ,  $\phi((0,1)) = (1,1)$ . Then  $\phi: \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z} \oplus \mathbb{Z}$   
 $(m,n) \mapsto (0,n)$ .

15. Find all ring hom<sup>s</sup>  $\phi: \mathbb{Z}_n \rightarrow \mathbb{Z}_k$ .

Solution: Group th<sup>y</sup>  $\Rightarrow k | n$ . If  $\phi: \mathbb{Z}_n \rightarrow \mathbb{Z}_k$  is a ring

hom<sup>s</sup>, then  $\phi([1]_n) = [1]_k \Rightarrow \forall [m]_n \in \mathbb{Z}_n$

$\phi: [m]_n \rightarrow [m]_k$ . Now, verify that  $\phi$  is a hom<sup>s</sup>.

$$\left. \begin{aligned} \phi([x]_n [y]_n) &= \phi([xy]_n) = [xy]_k \\ \phi([x]_n) \phi([y]_n) &= [x]_k [y]_k = [xy]_k \end{aligned} \right\} \Rightarrow \phi \text{ is a ring hom<sup>s</sup>.$$

(19) Let  $R = (\mathbb{Z}, \oplus, \odot)$  with  $m \oplus n = m+n-1$   
 $m \odot n = mn - mn$

Let  $\phi: \mathbb{Z} \rightarrow R$  have  $\phi(m) = 1-n$ . Show  $\phi$  is an isomorphism of rings.

Proof: Observe:  $\phi(0) = 1-0 = 1 = 0_R$  We also have:  
 $\phi(1) = 1-1 = 0 = 1_R$ .

•  $\phi(a+b) = 1-(a+b)$

$\phi(a) \oplus \phi(b) = (1-a) \oplus (1-b) = (1-a) + (1-b) - 1 = 1 - (a+b)$ .

•  $\phi(ab) = 1-ab$

$\phi(a) \odot \phi(b) = (1-a) \odot (1-b) = (1-a) + (1-b) - (1-a)(1-b)$   
 $= 1-ab$ .

Hence,  $\phi$  is a hom<sup>m</sup> of rings.

•  $\phi$  is onto:  $\forall n \in R, \phi(1-n) = 1 - (1-n) = n$ .

•  $\phi$  is 1-1.  $\ker \phi = \{r \in R : \phi(r) = 0_R = 1\} = \{0\}$

since  $\phi(r) = 1-r = 1 \Leftrightarrow r=0$ .

It follows that  $\phi$  is an isomorphism of rings.

(22) Let  $R$  be an integral domain. Show that  $\exists$  prime  $\mathfrak{p}$  such that  $R$  contains a subring isomorphic to  $\mathbb{Z}/\mathfrak{p} \iff \text{char}(R) = \mathfrak{p}$ .

Proof: Let  $\phi: \mathbb{Z} \rightarrow R$  such that  $\forall m \in \mathbb{Z}$ ,  
 $m \mapsto m \cdot 1_R$ .

Then  $\phi$  is a ring hom<sup>om</sup>:

$\cdot \phi(1) = 1$ ;  $\cdot \phi(a+b) = (a+b) \cdot 1_R = a \cdot 1_R + b \cdot 1_R = \phi(a) + \phi(b)$ ;

$\cdot \phi(ab) = ab \cdot 1_R = (a \cdot 1_R)(b \cdot 1_R) = \phi(a)\phi(b)$ .

Recall:

①  $\text{char}(R) = \text{prime } \mathfrak{p} \iff \mathfrak{p} \cdot 1_R = 0$ .

②  $\ker \phi \triangleleft \mathbb{Z}$ , a PID  $\implies \exists n \geq 0$  with  $\ker \phi = (n)$ .

Fund. Hom<sup>om</sup>. Th<sup>em</sup>.  $\implies \mathbb{Z}/\ker \phi \cong \mathbb{Z}/(n) \cong \mathbb{Z}/n$

$$\begin{array}{c} \mathbb{Z} \\ \downarrow \phi \\ \phi(\mathbb{Z}) \subseteq R \\ \uparrow \\ \text{subring} \end{array}$$

Now ① and ②  $\implies$  It suffices to show:  $\exists$  prime  $\mathfrak{p}$  with  $\mathfrak{p} \cdot 1_R = 0$ .

$\iff \ker \phi = (\mathfrak{p})$ .

( $\rightarrow$ ) Suppose:  $\exists$  prime  $p$  with  $p \cdot 1_R = 0$ .

Then  $p \in \ker \phi = (n) \Rightarrow n \mid p \Rightarrow n = 1$  or  $n = p$ .

If  $n = 1$ , then  $\ker \phi = (1) = \mathbb{Z} \Rightarrow \phi = 0 \Rightarrow \times$ .

Since  $\phi(1) = 1 \cdot 1_R = 1_R \neq 0_R$ . Hence,  $n = p$  and  $\ker \phi = (m) = (p)$ .

( $\Leftarrow$ ) Suppose  $\exists$  prime  $p$  with  $\ker \phi = (p)$ .

Then  $p \in \ker \phi \Rightarrow p \cdot 1_R = 0$ .

(23) Let  $R$  be an int. dom with  $\text{char}(R) = p > 0$ .

Show:  $\forall n \geq 1$  and all  $a, b \in R$ , we have  $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ .

Proof: We induct on  $n$ .

$$\underline{n=1}: (a+b)^p = \sum_{k=0}^p \binom{p}{k} a^{p-k} b^k$$

$\uparrow$   
 $R$ : commutative

Facts:  $p \mid \binom{p}{k} \Leftrightarrow 1 \leq k \leq p-1$ . Hence,  $\forall$  all such  $k$ ,  $\exists n_k \in \mathbb{Z}$

with  $n_k p = \binom{p}{k}$ . We have:  $(a+b)^p = \sum_{k=0}^p \binom{p}{k} a^{p-k} b^k$

$$= a^p + \sum_{k=1}^{p-1} n_k \underbrace{\left( p a^{p-k} b^k \right)}_{=0} + b^p = a^p + b^p.$$

$= 0$ :  $\text{char}(R) = p$

Done via fields.

induction step: For  $n \geq 1$  and suppose that

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}. \text{ Show: } (a+b)^{p^{n+1}} = a^{p^{n+1}} + b^{p^{n+1}}.$$

$$\text{We have: } (a+b)^{p^{n+1}} = [(a+b)^{p^n}]^p = (a^{p^n} + b^{p^n})^p$$

$$\stackrel{\substack{\uparrow \\ \text{ind. hyp}}}{=} a^{p^n \cdot p} + b^{p^n \cdot p} = a^{p^{n+1}} + b^{p^{n+1}}.$$

$\uparrow$   
base case