

MATH 4261(6261)

HW 3 SOLUTIONS TO THE HARDEST PROBLEMS

Section 4.2

**Problem 3.** If  $R$  is a finite integral domain show that  $R$  is a field.

**Solution.** First we show that  $R$  has an identity element for multiplication. To get started we claim that given  $a \in R$  there exists  $x_a \in R$  such that  $ax_a = a$ . Indeed, if  $a \neq 0$  the map  $T: R \rightarrow R$  defined by  $Tx = ax$  is easily shown to be one to one, and since  $R$  is finite it has to be onto. Hence, the equation  $ax = a$  has a solution. It remains to show that for nonzero  $a, b \in R$  we have  $x_a = x_b$ . Indeed, we have

$$0 = ab - ab = ax_a b - abx_b = ab(x_a - x_b)$$

and since  $R$  is an integral domain and  $ab \neq 0$  we get that  $x_a = x_b$ .

Denote by 1 the identity element for multiplication. Let  $a \in R$  nonzero. Since  $Tx = ax$  is onto, the equation  $ax = 1$  has a solution. As a result  $a$  has an inverse. (Alternatively we can argue as follows: Since  $R$  is finite, the elements  $a, a^2, \dots$  cannot be all distinct. Hence, there exist  $m, n \in \mathbb{N}$  with  $n > m$  such that  $a^n = a^m$ . This gives that  $a^n(a^{n-m} - 1) = 0$ , and since  $R$  is an integral domain and  $a \neq 0$ , we conclude that  $a^{n-m} = 1$ . Therefore, the inverse of  $a$  exists and is equal to  $a^{n-m-1}$ .)

**Problem 5.** Let  $R$  be a ring in which  $z^3 = z$  for every  $z \in R$ . Prove that  $R$  is commutative.

**Solution. 1st way.** To get started, we substitute  $z \rightarrow 2x$  in  $z^3 = z$  and use that  $x^3 = x$  to get that

$$(1) \quad 6x = 0.$$

Next substitute  $z \rightarrow x + y$  in the equation  $z^3 = z$ , expand, and use that  $x^3 = x$  and  $y^3 = y$  to get

$$(2) \quad x^2y + y^2x + xy^2 + yx^2 + xyx + yxy = 0.$$

Similarly, use the substitution  $z \rightarrow x - y$  (or just substitute  $y \rightarrow -y$  in (2)) to find that

$$(3) \quad -x^2y + y^2x + xy^2 - yx^2 - xyx + yxy = 0.$$

Adding (2) and (3) we get that

$$(4) \quad 2(y^2x + xy^2 + yxy) = 0.$$

We now multiply (4) on the left by  $y$ , and also on the right by  $y$ , and subtract the two equations. We get

$$(5) \quad 2(yx - xy) = 0.$$

Unfortunately, we are not done yet, we have to get rid of the 2 and this is not easy... To begin with we substitute  $y = x^2$  in (2). Since  $x^3 = x$  we find that

$$(6) \quad 3(x + x^2) = 0.$$

This equation looks helpful so we will exploit it more. We want to make the  $xy$  and  $yx$  appear, so we substitute  $x \rightarrow x + y$  in (6) and hope for the best! We get

$$3(x + y + x^2 + y^2 + xy + yx) = 0$$

and using that  $3(x + x^2) = 3(y + y^2) = 0$  (by (6)) this last equation gives that

$$(7) \quad 3(yx + xy) = 0.$$

This is good news, but we would prefer to have a  $-$  instead of a  $+$ . So remembering that from (1) we have  $6xy = 0$  and subtracting this from (8) we get

$$(8) \quad 3(yx - yx) = 0.$$

Now subtracting (5) from (8) gives that  $yx - xy = 0$ . Finished, at last!!

**2nd way.** This was given by one of your classmates.

First notice that if  $a = x^2$  then  $a^2 = x^4 = xx = a$ . So for  $a = x^2$  one considers the following identity (I cannot motivate it really)

$$(ay - aya)^2 = ayay - ayaya - aya^2y + aya^2ya = ayay - ayaya - ayay + ayay = 0.$$

This implies that  $ay - aya = 0$  (if  $z^2 = 0$  then  $z^3 = 0$  and so  $z = 0$  since  $z^3 = z$ ). So we have established that  $ay = aya$ . Similarly one gets  $ya = aya$ , and combining these two equations we get that  $ay = ya$  where  $a = x^2$ . Summarizing, we just showed that for  $x, y \in R$  we have

$$(9) \quad x^2y = yx^2$$

Now using repeatedly (9) for various values of  $x$  and  $y$  one gets

$$xy = (xy)^3 = xyxyxy = x(yx)^2y = (yx)^2xy = yxyx^2y = yxy^2x^2 = y^3x^3 = yx.$$

### Section 4.3

**Problem 25.** Let  $R$  be the ring of  $2 \times 2$  matrices over the real numbers; suppose that  $I$  is an ideal of  $R$ . Show that  $I = (0)$  or  $I = R$ .

**Solution.** If  $I \neq (0)$  then there exists a nonzero matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R$ . It suffices to show that  $I$  contains an invertible element  $A$ , since then  $I = A \times A^{-1} \in I$  and this

immediately implies that  $I = R$ . One way to do this is to left and right multiply the matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  with the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

A simple computation gives that the following matrices should belong to  $I$

$$\begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix}, \quad \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix}, \quad \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} b & d \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}.$$

Now we are almost done. Suppose that  $a \neq 0$ . Adding the third and fourth matrix we get that

$$\begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} = \begin{pmatrix} 0 & a \\ a & b+c \end{pmatrix} \in I.$$

Since the matrix  $\begin{pmatrix} 0 & a \\ a & b+c \end{pmatrix}$  is invertible, we have produced an invertible matrix in  $I$ . Similarly we treat the cases  $b, c$ , or  $d \neq 0$ .

#### Section 4.4

**Problem 3.** Let  $R = \{a + bi : a, b \in \mathbb{Z}\}$ . Show that  $M = \{x(2 + i) : x \in R\}$  is a maximal ideal of  $R$ .

**Solution.** Let  $M'$  be an ideal that strictly contains  $M$ . As usual our objective is to show that  $1 \in R'$ , since then  $M' = R$  and we are done. First notice that since  $(2 + i) \in M'$ , we have that  $5 = (2 - i)(2 + i) \in M'$ . Now take  $a + bi \in M' \setminus M$ . Since  $2a + ai = a(2 + i) \in M$ , it follows that  $(2b - a)i = 2(a + bi) - (2a + ai) \in M' \setminus M$ , which in turn implies that  $2b - a = (2b - a)i \cdot (-i) \in M' \setminus M$ . Since,  $5 \in M$  and  $2b - a \notin M$ , it follows that  $(2b - a, 5) = 1$ . But then  $1 = (2b - a)r + 5s$  for some  $s, t \in \mathbb{Z}$ , and since  $2b - a, 5 \in M'$ , we get that  $1 \in M'$ . This completes the proof.

**Problem 4.** If  $R$  and  $M$  are as in the previous problem, show that  $R/M \simeq \mathbb{Z}_5$ .

**Solution.** Our strategy is to use the first isomorphism theorem for rings. Define  $\phi: R \rightarrow \mathbb{Z}_5$  by  $\phi(a + bi) = [a - 2b]_5$ . It is a straightforward computation to show that  $\phi$  is a ring homomorphism which is onto  $\mathbb{Z}_5$ .

We claim that  $\ker \phi = M$ . If  $a + bi \in M$  then  $a = 2b$  and so  $\phi(a + bi) = 0$ . It follows that  $M \subset \ker \phi$ . On the other hand, suppose that  $a + bi \in \ker \phi$ . Then  $[a - 2b]_5 = [0]_5$ , or equivalently  $5|a - 2b$ . Hence,  $a = 2b + 5k$  for some  $k \in \mathbb{Z}$ , and so  $a + bi = b(2 + i) + 5k$ . Since  $b(2 + i) \in M$  and as we showed in the previous problem  $5k \in M$ , we get that  $a + bi \in M$ . This proves the inclusion  $\ker \phi \subset M$ , and completes the proof of the claim.

We can now apply the first homomorphism theorem for rings, it gives that  $R/M \simeq \mathbb{Z}_5$ .