

### Tutorial 3

1. Show that for any  $a$  in a ring  $R$ ,  $-(-a) = a$ .

Show that if the ring has an identity element 1,  $(-1)a = a(-1) = -a$ .

*Solution.*

By the defining property of negatives,  $a + (-a) = 0$ . Adding  $-(-a)$  to both sides deduce  $a = -(-a)$ . Multiplying  $1 + (-1) = 0$  on the left by  $a$  and using the distributive law and definition of 1, gives  $a + (-1)a = 0$ . Adding  $-a$  to each side gives  $(-1)a = -a$ . Similarly multiplying  $1 + (-1) = 0$  on the right by  $a$  gives  $a(-1) = -a$ .

2. (*The Cancellation Law for Integral Domains*). Let  $R$  be an integral domain and  $a, b, c \in R$ . Suppose  $ab = ac$  and  $a \neq 0$ . Prove that  $b = c$ .

*Solution.*

As  $R$  an integral domain it has no zero divisors, i.e.  $xy = 0$  in  $R$  implies  $x = 0$  or  $y = 0$ . If  $ab = ac$ , then  $a(b - c) = 0$ . So  $a \neq 0$  implies  $b - c = 0$ , i.e.  $b = c$ .

3. Show that if  $R$  and  $S$  are integral domains, and  $\phi: R \rightarrow S$  is a ring homomorphism, then either  $\phi(x) = 0$  for all  $x \in R$ , or else  $\phi$  takes the identity element of  $R$  to the identity element of  $S$ .

*Solution.*

Let  $1_R$  and  $1_S$  denote the identity elements of  $R$  and  $S$ . Suppose that there exists  $x \in R$  with  $\phi(x) \neq 0$ . Then for this value of  $x$  we have

$$\phi(x)1_S = \phi(x) = \phi(x1_R) = \phi(x)\phi(1_R),$$

and, cancelling the nonzero element  $\phi(x)$  (valid by Exercise 2), it follows that  $1_S = \phi(1_R)$ .

4. Suppose  $\phi: R \rightarrow S$  is a ring homomorphism. Show  $\ker \phi = \{0\}$  if and only if  $\phi$  is injective.

*Solution.*

See Unit Notes Proposition 5.14.

5. Let  $I$  and  $J$  be ideals in the ring  $R$ .

- (i) Define  $I + J = \{x + y \mid x \in I \text{ and } y \in J\}$ . Prove that  $I + J$  is an ideal in  $R$ .  
 (ii) Prove that  $I \cap J$  is an ideal in  $R$ .  
 (iii) Define  $IJ = \{\sum_{k=1}^n a_k b_k \mid n \in \mathbb{N}, \text{ and } a_k \in I, b_k \in J \text{ for all } k\}$ . Prove that  $IJ$  is an ideal in  $R$ , and that  $IJ \subseteq I \cap J$ .

*Solution.*

- (i) Since  $I$  and  $J$  are ideals they are nonempty; so there exists at least one element  $x_0 \in I$  and at least one element  $y_0 \in J$ . Since  $x_0 + y_0 \in I + J$  it follows that  $I + J \neq \emptyset$ . (In fact, we showed in lectures that a subring must always contain the zero element of the ring; so we could take  $x_0 = y_0 = 0$ .)

Let  $a, b \in I + J$  and  $r \in R$ . Then  $a = x + y$  and  $b = z + w$  for some  $x, z \in I$  and  $y, w \in J$ . Using various ring axioms and trivial consequences of the ring axioms we find that

$$a + b = (x + y) + (z + w) = (x + z) + (y + w),$$

$$-a = -(x + y) = (-x) + (-y),$$

$$ra = r(x + y) = rx + ry,$$

and

$$ar = (x + y)r = xr + yr.$$

Now since  $I$  is an ideal it is closed under addition, finding negatives, and multiplication by elements of  $R$ , and so it follows that  $x + z$ ,  $-x$ ,  $rx$  and  $xr$  are all elements of  $I$ . Similarly  $y + w$ ,  $-y$ ,  $ry$  and  $yr$  are in  $J$ . So

$$a + b = (x + z) + (y + w) \in I + J,$$

and similarly  $-a$ ,  $ra$  and  $ar$  are in  $I + J$ . So  $I + J$  is closed under addition, finding negatives and multiplying by elements of  $R$ . Hence  $I + J$  is an ideal.

- (ii) Since  $0 \in I$  and  $0 \in J$  it follows that  $0 \in I \cap J$ , which is therefore nonempty. Let  $x, y \in I \cap J$  and  $r \in R$ . Then  $x, y \in I$  (since  $I \cap J \subseteq I$ ) and  $x, y \in J$  (since  $I \cap J \subseteq J$ ) and so the closure properties of  $I$  and  $J$  yield that  $x + y$ ,  $-x$ ,  $rx$ ,  $xr \in I$  and  $x + y$ ,  $-x$ ,  $rx$ ,  $xr \in J$ . Hence it follows that  $x + y$ ,  $-x$ ,  $rx$ ,  $xr \in I \cap J$ , and so  $I \cap J$  satisfies all the requisite closure properties. So  $I \cap J$  is an ideal.

- (iii) Choose  $n = 1$  and choose an element  $a_1 \in I$  and an element  $b_1 \in J$ . (This can be done since  $I \neq \emptyset$  and  $J \neq \emptyset$ .) Then  $a_1 b_1 = \sum_{k=1}^1 a_k b_k$  is an element of  $IJ$ ; hence  $IJ \neq \emptyset$ .

Let  $x, y \in IJ$  and  $r \in R$ . Then there exist  $n, m \in \mathbb{N}$  and elements  $a_k, c_l \in I$  and  $b_k, d_l \in J$  (for  $1 \leq k \leq n$  and  $1 \leq l \leq m$ ) such that  $x = \sum_{k=1}^n a_k b_k$  and  $y = \sum_{l=1}^m c_l d_l$ . We find that

$$x + y = \sum_{k=1}^n a_k b_k + \sum_{l=1}^m c_l d_l = \sum_{p=1}^{n+m} e_p f_p$$

where the  $e_p$  are elements of  $I$  and the  $f_p$  elements of  $J$  defined by

$$e_p = \begin{cases} a_p, & \text{for } 1 \leq p \leq n \\ c_{p-n}, & \text{for } n+1 \leq p \leq n+m \end{cases}$$

$$f_p = \begin{cases} b_p & \text{for } 1 \leq p \leq n \\ d_{p-n} & \text{for } n+1 \leq p \leq n+m. \end{cases}$$

So  $x + y \in IJ$ . Furthermore,

$$-x = -\sum_{k=1}^n a_k b_k = \sum_{k=1}^n (-a_k) b_k,$$

$$rx = r \sum_{k=1}^n a_k b_k = \sum_{k=1}^n (ra_k) b_k,$$

$$xr = \left( \sum_{k=1}^n a_k b_k \right) r = \sum_{k=1}^n a_k (b_k r),$$

and these are all in  $IJ$  since  $-a_k, ra_k \in I$  and  $b_k r \in J$  for all values of  $k$  (by the closure properties of the ideals  $I$  and  $J$ ). So  $IJ$  satisfies all the necessary closure properties and is therefore an ideal.

Let  $t \in IJ$ . Then  $t = \sum_{k=1}^n a_k b_k$  for some  $n \in \mathbb{N}$  and some elements  $a_k \in I$  and  $b_k \in J$ . Since  $I$  is closed under multiplication by arbitrary elements of  $R$  the fact that  $a_k \in I$  ensures that  $a_k b_k \in I$ , for each  $k$ . Since  $I$  is closed under addition,  $\sum_{k=1}^n a_k b_k \in I$ . Similarly,  $b_k \in J$  gives  $a_k b_k \in J$  for all  $k$ , and hence  $\sum_{k=1}^n a_k b_k \in J$ . So  $t$  is in both  $I$  and  $J$ , and since  $t$  was arbitrary it follows that  $IJ \subseteq I \cap J$ .

6. Determine  $I + J, I \cap J, IJ$  for the ideals  $I = 84\mathbb{Z}$  and  $J = 90\mathbb{Z}$  in the ring  $\mathbb{Z}$ .

*Solution.*

$I + J = 6\mathbb{Z}$ ,  $I \cap J = 1260\mathbb{Z}$ ,  $IJ = 7560\mathbb{Z}$ . Note 6 is the greatest common divisor of 84 and 90, 1260 their lowest common multiple and  $7560 = 84 \times 90 = 6 \times 1260$  their product.

7. (i) Let  $R$  be a ring with 1. An element  $u \in R$  is called a *unit* if there exists a  $v \in R$  such that  $uv = vu = 1$ . Show that if  $I$  is an ideal of  $R$  and some element  $x \in I$  is a unit then  $I = R$ .
- (ii) Let  $F$  be a field and  $I$  an ideal in  $F$ . Prove that either  $I = \{0\}$  or  $I = F$ .
- (iii) Show that a commutative ring  $F$  with identity which has exactly two ideals  $\{0\}$  and  $F$  is a field.

*Solution.*

- (i) Let  $x \in I$  be a unit in  $R$ . Then we may choose  $y \in R$  be such that  $xy = 1$ . Now if  $r$  is an arbitrary element of  $R$ , we have

$$r = 1r = (xy)r = x(yr)$$

which is an element of  $I$  since  $x \in I$  and  $I$  is closed under right multiplication by elements of  $R$ . So all elements of  $R$  are in  $I$ , and since  $I$  is by definition a subset of  $R$  it follows that  $I = R$ .

- (ii) Suppose that  $I \neq \{0\}$ . Then since  $I \neq \emptyset$  (since ideals are subrings and hence must contain at least a zero element) it follows that there exists  $x \in I$  with  $x \neq 0$ . Since  $F$  is a field all nonzero elements have inverses; that is, all nonzero elements of  $F$  are units. Since  $I$  contains the unit  $x$  it follows by Part (i) that  $I = F$ .
- (iii) Since  $F \neq \{0\}$ ,  $F$  is not the zero ring. Since we are given it is a commutative ring it remains to show each  $x \neq 0$  has a multiplicative inverse. Suppose  $x \neq 0$ . Then  $xF$ , all multiples of  $x$ , is an ideal of  $F$ .  $xF \neq \{0\}$  because  $x = x1 \in F$ . Hence we must have  $xF = F$ . Hence  $1 = xy$  for some  $y \in F$ . This  $y$  is a multiplicative inverse for  $x$ .

8. Let  $I$  be a nonzero ideal in the ring  $M_2(\mathbb{Q})$ , and  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  a nonzero element of  $I$ .

- (i) Prove that  $I$  contains the elements  $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix}$ .
- (ii) Prove that  $I$  contains  $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ .
- (iii) Prove that  $I = M_2(\mathbb{Q})$ .

Using a similar procedure, can you find all the ideals in the ring  $M_2(\mathbb{Z})$ ?

*Solution.*

For example,  $\begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I$  since one of the factors is in  $I$ . As  $I$  contains some  $\begin{pmatrix} t & 0 \\ 0 & 0 \end{pmatrix}$  with  $t \neq 0$ , it must contain  $\begin{pmatrix} t^{-1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ , and indeed all matrices of the form  $\begin{pmatrix} p & 0 \\ 0 & 0 \end{pmatrix}$ . Similarly  $I$  contains all matrices of the form  $\begin{pmatrix} 0 & q \\ 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 0 \\ r & 0 \end{pmatrix}$  and  $\begin{pmatrix} 0 & 0 \\ 0 & s \end{pmatrix}$ . Adding these shows that  $I$  contains all matrices.

By the same arguments as above, if  $I$  is any ideal in  $M_2(\mathbb{Z})$  and  $t$  is any entry of any matrix in  $I$ , then the matrix  $\begin{pmatrix} t & 0 \\ 0 & 0 \end{pmatrix}$  is in  $I$ . Define

$$L = \{t \in \mathbb{Z} \mid \begin{pmatrix} t & 0 \\ 0 & 0 \end{pmatrix} \in I\}.$$

Since  $I$  is closed under addition, negatives and multiplication by arbitrary elements of  $M_2(\mathbb{Z})$ , it is easily seen that  $L$  is closed under addition, negatives and multiplication

by arbitrary elements of  $\mathbb{Z}$  (as well as being nonempty). So  $L$  is an ideal in  $\mathbb{Z}$ . And if  $p, q, r, s \in L$  then

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} p & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} q & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} s & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in I,$$

and so it follows that  $I = \left\{ \begin{pmatrix} p & q \\ r & s \end{pmatrix} \mid p, q, r, s \in L \right\}$ . In other words, every ideal in  $M_2(\mathbb{Z})$  has the form  $M_2(L)$  where  $L$  is an ideal in  $\mathbb{Z}$ , that is,  $L = d\mathbb{Z}$  for some integer  $d$ .