# MATH321 Tutorial 1

Emma Hogan

53837798

February 24, 2020

#### Question 1

Let d be an integer. Show that  $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$  is an integral domain.

First, observe  $\mathbb{Z}[\sqrt{d}]$  is a ring because it is a subset of  $\mathbb{C}$  that is non-empty (as  $a, b \in \mathbb{Z} \neq \phi$ ), and  $\forall a_1, a_2, b_1, b_2 \in \mathbb{Z}[\sqrt{d}]$  it is:

1) Closed under subtraction:

$$(a_1 + b_1\sqrt{d}) - (a_2 + b_2\sqrt{d}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$$

2) Closed under multiplication:

$$(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + b_1a_2)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$$

[Note:  $ab, a - b \in \mathbb{Z} \ \forall \ a, b \in \mathbb{Z}$ ]

Now, with  $a=1,\,b=0$  we have e=1 in  $\mathbb{Z}[\sqrt{d}]$  such that  $\forall \ a+b\sqrt{d}\in\mathbb{Z}[\sqrt{d}]$ :

$$e(a+b\sqrt{d}) = (a+b\sqrt{d})e = (a+b\sqrt{d})$$

So,  $\mathbb{Z}[\sqrt{d}]$  has a unity. Also, since we have shown  $\mathbb{Z}[\sqrt{d}]$  is a subring of  $\mathbb{C}$  and  $\mathbb{C}$  does not have any zero divisors,  $\mathbb{Z}[\sqrt{d}]$  also can not have any zero divisors.

Therefore, as  $\mathbb{Z}[\sqrt{d}]$  is a ring with unity and no zero divisors, it is an integral domain.

## Question 2

### Find all units and zero-divisors in the ring $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ .

Since addition and multiplication in  $\mathbb{Z}_4 \oplus \mathbb{Z}_4$  are performed pointwise, we need to find units and zero divisors in  $\mathbb{Z}_4$  and  $\mathbb{Z}_3$  and pair them up, and then consider the zeros of each.

The units of  $\mathbb{Z}_4$  and  $\mathbb{Z}_3$  are precisely those elements relatively prime to 4 and 3 respectively.

 $\mathbb{Z}_4$  units =  $\{1,3\}$  $\mathbb{Z}_3$  units =  $\{1,2\}$ 

Adding the zeros of to the possible combinations, we get the units of  $\mathbb{Z}_4 \oplus \mathbb{Z}_4$  are (1,1), (1,2), (3,1), (3,2), (0,1), (0,2), (1,0) and (3,0).

Similarly, by constructing Cayley tables we can observe that  $\mathbb{Z}_4$  has a zero-divisor of 2, and  $\mathbb{Z}_3$  has no zero-divisors. Thus, the only zero-divisor of  $\mathbb{Z}_4 \oplus \mathbb{Z}_4$  is (2,0).

#### Question 3

#### Prove or disprove that

(a) 
$$R = \left\{ \begin{bmatrix} 0 & a \\ b & a \end{bmatrix} | a, b, c \in \mathbb{Q} \right\}$$

(b) 
$$S_d = \left\{ \begin{bmatrix} a & bd \\ b & c \end{bmatrix} | a, b \in \mathbb{R} \right\}$$

is a subring of the matrix ring  $M_2(\mathbb{R})$ , where d is an arbitrary (but fixed) integer.

(a) This fails the subring test:

Let  $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathbb{Q}$ .

$$\left[\begin{array}{cc} 0 & a_1 \\ b_1 & c_1 \end{array}\right] \left[\begin{array}{cc} 0 & a_2 \\ b_2 & c_2 \end{array}\right] = \left[\begin{array}{cc} a_1b_2 & a_1c_1 \\ c_1b_2 & b_1a_2 + c_1c_2 \end{array}\right] \notin R.$$

So R is not a subring of  $M_2(\mathbb{R})$  as it is not closed under multiplication.

(b) Again we apply the subring test.  $S_d$  is clearly non-empty, so take  $a_1, a_2, b_1, b_2 \in \mathbb{R}, d \in \mathbb{Z}$ .

$$\begin{bmatrix} a_1 & b_1 d \\ b_1 & a_1 \end{bmatrix} - \begin{bmatrix} a_2 & b_2 d \\ b_2 & a_2 \end{bmatrix} = \begin{bmatrix} a_1 - a_2 & b_1 d - b_2 d \\ b_1 - b_2 & a_1 - a_2 \end{bmatrix} \in S_d$$

So  $S_d$  is closed under subtraction.

$$\left[\begin{array}{cc} a_1 & b_1d \\ b_1 & a_1 \end{array}\right] * \left[\begin{array}{cc} a_2 & b_2d \\ b_2 & a_2 \end{array}\right] = \left[\begin{array}{cc} a_1a_2 + b_1db_2 & a_1b_2d + b_1da_2 \\ b_1a_2 + a_1b_2 & a_1a_2 + b_1b_2d \end{array}\right] = \left[\begin{array}{cc} a_1a_2 + b_1b_2d & (a_1b_2 + b_1a_2)d \\ a_1b_2 + b_1a_2 & a_1a_2 + b_1b_2d \end{array}\right] \in S_d$$

(By taking  $a = a_1a_2 + b_1b_2d$ ,  $b = a_1b_2 + b_1a_2$ )

So  $S_d$  is closed under multiplication as well, and is therefore a subring of  $M_2(\mathbb{R})$ .

# Question 4

Find units and zero divisors in the RING examples in Q3. Do you find them all? Does the answer depend on the value of d?

The units of  $\mathcal{S}_d$  are the invertible matrices of the form

$$\left[\begin{array}{cc} a & bd \\ b & a \end{array}\right]$$

These are invertible when

$$a^{2} - b^{2}d \neq 0$$
$$a^{2} \neq b^{2}d$$
$$a \neq \pm b\sqrt{d}$$

Zero-divisors are any elements

$$\left[\begin{array}{cc} a_1 & b_1 d \\ b_1 & a_1 \end{array}\right]$$

2

Such that for some  $a_2, b_2 \in \mathbb{R}$ 

$$\left[\begin{array}{cc} a_1 & b_1 d \\ b_1 & a_1 \end{array}\right] * \left[\begin{array}{cc} a_2 & b_2 d \\ b_2 & a_2 \end{array}\right] = \left[\begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array}\right]$$

I'm too lazy to solve simultaneous equations or mess around with null spaces, so instead I will take a shortcut by observing that zero-divisors can never be units. So, by the working earlier used to classify units, we know that all zero divisors must have  $a = \pm b\sqrt(d)$ . Note this is a sufficient but not necessary condition for the zero divisor, so we are not done. We have however, eliminated some variables.

By substituting  $a_1 = \pm b_1 \sqrt(d)$  and  $a_2 = \pm b_2 \sqrt(d)$  into the product calculated earlier and solving each entry for 0, we find that for any matrix of the form

$$\begin{bmatrix}
\pm b_1 \sqrt{(d)} & b_1 d \\
b_1 & \pm b_1 \sqrt{(d)}
\end{bmatrix}$$

We can calculate  $a_2 = \mp b_2 \sqrt{(d)}$  and find a matrix of the form

$$\left[\begin{array}{cc} \mp b_2 \sqrt(d) & b_2 d \\ b_2 & \mp b_2 \sqrt(d) \end{array}\right]$$

And their product will be 0 as shown.

$$\left[\begin{array}{cc} \pm b_1\sqrt(d) & b_1d \\ b_1 & \pm b_1\sqrt(d) \end{array}\right] * \left[\begin{array}{cc} \mp b_2\sqrt(d) & b_2d \\ b_2 & \mp b_2\sqrt(d) \end{array}\right] = \left[\begin{array}{cc} -b_1b_2d + b_1b_2d & \mp b_1b_2d\sqrt{d} \pm b_1b_2d\sqrt{d} \\ \mp b_1b_2\sqrt{d} \pm b_1b_2\sqrt{d} & b_1b_2d - b_1b_2d \end{array}\right] = \left[\begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array}\right]$$

The condition on d is that  $S_d$  is only defined over the reals, so  $d \ge 0$ . If d < 0 then every element in  $S_d$  is invertible, and there are no zero-divisors.

Interestingly, despite me saying not being a unit was only a necessary condition for being a zero-divisor, in this ring it turned out to be sufficient. I have not convinced myself of a reason why this is the case - the ring is commutative, but not finite so the result shown in class doesn't apply. I feel like I'm missing something.