

# MA151 Algebra 1, Assignment 4

Dyson Dyson

## Question 1

Let  $R$  be a non-zero ring. Let  $a \sim b$  be the relation “ $a$  is an associate of  $b$ ”, meaning there exists a unit  $v \in R$  such that  $av = b$ .

### Q1 (a)

Prove that  $a \sim b$  is an equivalence relation on  $R$ .

An equivalence relation is reflexive, transitive, and symmetric.

For reflexivity, if  $a \sim b$ , then  $\exists v \in R$  such that  $av = b$  and  $v$  is a unit. Then  $avv^{-1} = bv^{-1} \implies bv^{-1} = a$ , so  $b \sim a$ .

Now for transitivity, suppose  $a \sim b$  and  $b \sim c$ , so  $\exists v, u \in R$  such that  $av = b$  and  $bu = c$ . Then  $(av)u = bu = c \implies a(vu) = c$ , so  $a \sim c$ .

And for symmetry,  $a1 = a$ , so  $a \sim a$ .

Therefore this is an equivalence relation.

### Q1 (b)

Describe the equivalence classes in the case  $R = \mathbb{Z}$ .

The only units in  $\mathbb{Z}$  are  $\{1, -1\}$ , so  $a \sim b$  if and only if  $a = b$  or  $a = -b$ . Therefore 0 is equivalent to nothing, and every positive integer  $x$  gets the equivalence class  $[x]_{\sim} = \{x, -x\}$ .

## Question 2

Let  $R$  be a ring and let  $a \in R$ .

### Q2 (a)

Show that if  $R$  is commutative,  $aR = \{ar \mid r \in R\}$  is an ideal of  $R$ .

For  $aR$  to be an ideal of  $R$ , we need  $(aR, +)$  to be a subgroup of  $(R, +)$ , and we need  $xy \in aR$  and  $yx \in aR$  for all  $x \in R$ ,  $y \in aR$ . Since  $R$  is commutative, we only need to worry about one of these.

First, the ABC test for subgroups. The identity in  $(R, +)$  is just 0, which is trivially in  $aR$ . The sum of two terms  $ar_1$  and  $ar_2$  is  $a(r_1 + r_2)$ . Clearly  $r_1 + r_2 \in R$ , so  $a(r_1 + r_2) \in aR$ . The inverse of an element  $ar$  is just  $-ar = a(-r)$ , and  $-r \in R$ , so  $-ar \in aR$ . Therefore  $(aR, +)$  is a subgroup of  $(R, +)$ .

Now consider an arbitrary element  $ar \in aR$  and an arbitrary element  $x \in R$ . Their product is  $arx = a(rx)$ , and since  $rx \in R$ ,  $a(rx) \in aR$ . Therefore  $aR$  is an ideal of  $R$ .

### Q2 (b)

Show by an example that this may be false if  $R$  is not commutative.

Choose  $R = GL_2(\mathbb{R})$  and  $a = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ . Then right-multiplying an element of  $aR$  by an element of  $R$  would keep the result in  $aR$ , but left-multiplying wouldn't necessarily. Therefore  $aR$  is not an ideal of  $R$  in this case.

### Question 3

#### Q3 (a)

List the elements of  $(\mathbb{Z}/7\mathbb{Z})^*$ , the group of units in the ring  $\mathbb{Z}/7\mathbb{Z}$ .

$$(\mathbb{Z}/7\mathbb{Z})^* = \{1, 2, 3, 4, 5, 6\}$$

#### Q3 (b)

List the elements of  $(\mathbb{Z}/8\mathbb{Z})^*$ , the group of units in the ring  $\mathbb{Z}/8\mathbb{Z}$ .

$$(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$$

#### Q3 (c)

Show that  $((\mathbb{Z}/7\mathbb{Z})^*, \times_7)$  is a cyclic group but  $((\mathbb{Z}/8\mathbb{Z})^*, \times_8)$  is not a cyclic group.

We shall just draw the Cayley tables for these groups.

First,  $(\mathbb{Z}/7\mathbb{Z})^*$ ,

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

And then,  $(\mathbb{Z}/8\mathbb{Z})^*$ ,

$\times_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Just from looking at these tables, we can deduce that  $((\mathbb{Z}/7\mathbb{Z})^*, \times_7) \cong C_6$  and  $((\mathbb{Z}/8\mathbb{Z})^*, \times_8) \cong K_4$ . But  $K_4$  is not cyclic, so  $((\mathbb{Z}/8\mathbb{Z})^*, \times_8)$  is not cyclic.

## Question 4

Let  $R = M_{2 \times 2}(\mathbb{Q})$ , the ring of  $2 \times 2$  matrices with rational entries under matrix addition and multiplication. Show that the only ideals of  $R$  are  $\{\mathbf{0}\}$  and  $R$ .

Let  $\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ . If an ideal of  $R$  did not contain  $\mathbf{0}$ , then it wouldn't be a subgroup under addition because it wouldn't have an additive identity. Therefore every ideal needs  $\mathbf{0}$ . Also note that  $\{\mathbf{0}\}$  is itself an ideal of  $R$ , since multiplying by anything from  $R$  just results in  $\mathbf{0}$  again.

Now suppose we have some ideal  $I$  containing  $\mathbf{0}$  and some  $X \neq \mathbf{0}$ . Since  $(I, +)$  is a group, it must also contain all integer multiples of  $X$ . And since  $mX \in I$  and  $Xm \in I$  for all  $m \in R$ ,  $I$  must expand to include all of  $R$ .

To see this, we can imagine an arbitrary “target” matrix  $t \in R$ , then find the matrix  $m$  such that  $Xm = t$ . Let  $X = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ ,  $m = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ , and  $t = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ . Then

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$px + ry = a$$

$$qx + sy = b$$

$$pz + rw = c$$

$$qz + sw = d$$

Since  $x, y, z, w, a, b, c, d$  are all known, these equations can always be solved for  $p, q, r, s$ . Therefore  $\forall t \in R, \exists m \in R$  such that  $Xm = t$ . Therefore  $I$  must contain all elements of  $R$ , so  $I = R$ .

Therefore the only ideals of  $R$  are  $\{\mathbf{0}\}$  and  $R$ .

## Question 5

Let  $R = \mathbb{R}[x]$ , the ring of polynomials with real coefficients. Let

$$I = \{f(x) \in \mathbb{R}[x] \mid f(0) = 0\}.$$

### Q5 (a)

Show that  $I$  is an ideal of  $R$  with  $I \neq R$ .

Clearly  $I \neq R$ , since there exists polynomials in  $f(x) \in \mathbb{R}[x]$  where  $f(0) \neq 0$ . Take  $f(x) = x^2 + 1$ , for instance. In this case,  $f(0) = 1$ . Therefore  $I \neq R$ .

For  $I$  to be an ideal of  $R$ , we need  $(I, +)$  to be a subgroup of  $(R, +)$ , for which we will use the ABC test, and we need  $ir \in I$  and  $ri \in I$  for all  $r \in R, i \in I$ , but multiplication is commutative here, so we only need to worry about one of these.

First, the ABC test for subgroups. The identity in  $(R, +)$  is just 0, which is trivially in  $I$ . The sum of two polynomials with zero constant term is another polynomial with zero constant term, so the sum of two elements in  $I$  is another element in  $I$ . And the inverse of a polynomial with zero constant term is the negative version of that polynomial, which also has zero constant term, so  $(I, +)$  has inverses. Therefore  $(I, +)$  is a subgroup of  $(R, +)$ .

Now consider an arbitrary polynomial  $r$  from  $\mathbb{R}[x]$  and an arbitrary polynomial  $i$  from  $I$ . To find the constant term of their product, we just find the product of their constant terms. Since  $i$  has a constant term of 0,  $ri$  and  $ir$  both have a constant term of 0, so are both members of  $I$ .

Therefore  $I$  is an ideal of  $R$ .

### Q5 (b)

Prove that if  $J$  is an ideal of  $R$  with  $I \subsetneq J$  then  $J = R$ .

Since  $I$  definitionally includes all polynomials with zero constant term,  $J$  must include at least one polynomial with non-zero constant term. Without loss of generality, assume we have some  $j(x) \in J$  where  $j(0) = a$  and  $a \neq 0$ . Then for  $J$  to be an ideal of  $R$ , we need  $r(x)j(x) \in J$  and  $j(x)r(x) \in J$  for all  $x \in R$ , although multiplication is commutative here, so we only need to worry about one of these.

Since  $r(x)$  could be any element from  $\mathbb{R}[x]$ , we will end up generating all of  $\mathbb{R}[x]$ . We know that  $J$  already contains every combination of real coefficients for powers of  $x$ , but we only know that it contains constant term  $a$ . But we can obtain any constant term  $b$  by multiplying by some particular  $r(x)$  with

$r(0) = \frac{b}{a}$ , since  $j(0) = a$  and  $a \neq 0$ . Then  $r(0)j(0) = b$ , so  $J$  must contain polynomials that cover all real constant terms.

Thus,  $J$  must contain every polynomial from  $\mathbb{R}[x]$ , so  $J = R$ .

## Question 6

### Q6 (a)

Show that  $x^3 + x^2 + x + 1$  is not irreducible over  $\mathbb{Q}$ .

$$x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$$

### Q6 (b)

Show that  $x^4 + 1$  is irreducible over  $\mathbb{Q}$  but not irreducible over  $\mathbb{R}$ .

Let  $f(x) = x^4 + 1$ . We can use Eisenstein's criterion to show that  $f(x)$  is irreducible over  $\mathbb{Q}$ , recalling the fact that  $f(x)$  is irreducible if and only if  $f(x+1)$  is irreducible. In this case  $f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$ .

Now we will choose our prime  $p = 2$ .  $p$  divides all the coefficients, excluding the coefficient of the term with the highest degree.  $p \nmid 1$ , and  $p^2 \nmid 2$ . Therefore  $f(x+1)$  fulfils Eisenstein's criterion and is therefore irreducible over  $\mathbb{Q}$ . Therefore  $f(x)$  is irreducible over  $\mathbb{Q}$ .

But  $x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$ , so  $f(x)$  is not irreducible over  $\mathbb{R}$ .

### Q6 (c)

Show that  $x^2 + x + 4$  is irreducible over  $\mathbb{Z}/11\mathbb{Z}$ . Here any coefficients should be interpreted modulo 11.

Let  $f(x) = x^2 + x + 4$ . If  $f(x)$  were not irreducible over  $\mathbb{Z}/11\mathbb{Z}$ , then we could write  $x^2 + x + 4 = (ax + b)(cx + d) = acx^2 + (ad + bc)x + bd$ , which gives the following system of equations,

$$\begin{aligned} ac &\equiv 1 \\ ad + bc &\equiv 1 \\ bd &\equiv 4 \end{aligned}$$

And then I get stuck.

**Q6 (d)**

Show that  $x^4 + 1$  is not irreducible over  $\mathbb{Z}/5\mathbb{Z}$ . Here any coefficients should be interpreted modulo 5.

Consider  $f(x) = x^4 + 1$ . The question says this is not irreducible over  $\mathbb{Z}/5\mathbb{Z}$ , but I don't know why. I can't find a root modulo 5, so it has no linear factors, but factoring into two quadratics doesn't seem to work either because I get two simultaneous equations mod 5 and nothing satisfies both.