# MAT220 manditory 2

Fromsa

March 12, 2018

1. R with the given operation is a ring if these criteria are met.
   Let $(a,b),(c,d)$ and $(e,f) \in R$

   - **Closed under addition**
     Since $a,b,c,d \in \mathbb{Z}_2$, we have that $(a+c) \in \mathbb{Z}_2$ and $(b+d) \in \mathbb{Z}_2$ and thus $(a,b) \oplus (c,d) = (a+c, b+d) \in \mathbb{Z}_2 \times \mathbb{Z}_2 = R$ ✓
   - **Associative addition**
     $(a,b) \oplus ((c,d) \oplus (e,f)) = (a,b) \oplus (c+e, d+f) = ((a+(c+e)),(b+(d+f)) := L$
     by associative addition of $\mathbb{Z}_2$ we have that
     $L = ((a+c)+e,(b+d)+f)$
     $= ((a+c),(b,d)) \oplus (e,f)$
     $= ((a,b) \oplus (c,d)) \oplus (e,f)$ ✓
   - **Commutative addition**
     $(a,b) \oplus (c,d) = (a+c, b+d) := L$ by commutative addition of $\mathbb{Z}_2$ we have that
     $L = (c+a, d+b) = (c,d) \oplus (a,b)$ ✓
   - **Additive identity/ zero element**
     Assume $(0,0) = 0_R$
     - $(a,b) \oplus (0,0) = (a+0, b+0) := L$ by $0_{\mathbb{Z}_2} = 0$ we have that $L = (a,b)$
     - $(0,0) \oplus (a,b) = (0+a, 0+b) := L$ by $0_{\mathbb{Z}_2} = 0$ we have that $L = (a,b)$

     ✓
   - **Closer under subtraction***
     $(a,b) \oplus (x,y) = (0,0) \iff (a+x, b+y) = (0,0)$ by $\mathbb{Z}_2$ we have
     $a + x = 0 \iff x = -a = a \in \mathbb{Z}_2$
     and
     $b + y = 0 \iff y = -b = b \in \mathbb{Z}_2$ ✓
   - **Closed under multiplication**
     $(a,b) \odot (c,d) = (ac, ad+bc)$
     by closer of multiplication of $\mathbb{Z}_2$ we have that $ac \in \mathbb{Z}_2$ and by also closer of addition of $\mathbb{Z}_2$ we have $ad+bc \in \mathbb{Z}_2$ and therefore is $(a,b) \odot (c,d) \in R$ ✓
   - **Associative multiplication**
     $(a,b) \odot ((d,c) \odot (e,f)) = (a,b) \odot (de, df+ce) = (a(de), a(df+ce)+b(de)) := L$
     by Associative multiplication of $\mathbb{Z}_2$ we have
     $L = (e(ad), a(df) + a(ce) + e(bd))$
     $= (e(ad), (ad)f + (ac)e + e(bd))$
     $= (e(ad), f(ad) + e(ac+bd))$
     $= (ad, ac+bd) \odot (e,f)$
     $= ((a,b) \odot (c,d)) \odot (e,f)$ ✓
   - **Distributive law**

     - $(a,b) \odot ((c,d) \oplus (e,f))$
       $= (a,b) \odot (c+e, d+f)$

$$= (a(c+e), a(d+f) + b(c+e))$$
$$= (ac+ae, (ad+af) + (bc+be))$$
$$= (ac+ae, (ad+bc) + (af+be))$$
$$= (ac, (ad+bc)) \oplus (ae, af+be)$$
$$= ((a,b) \odot (c,d)) \oplus ((a,b) \odot (e,f))$$

– $((a,b) \oplus (c,d)) \odot (e,f)$
$$= (a+c, b+d) \odot (e,f)$$
$$= ((a+c)e, (a+c)f + (b+d)e)$$
$$= ((ae+ce), (af+cf) + (be+de))$$
$$= (ae+ce, (af+be) + (cf+de))$$
$$= (ae, af+be) \oplus (ce, (cf+de))$$
$$= ((a,b) \odot (e,f) \oplus ((c,d) \odot (e,f))$$

✓

$\therefore$ R is a ring with the given operations. □

2. –

Addition table for $R$

| + | (0,0) | (0,1) | (1,0) | (1,1) |
|---|---|---|---|---|
| (0,0) | (0,0) | (0,1) | (1,0) | (1,1) |
| (0,1) | (0,1) | (0,0) | (1,1) | (1,0) |
| (1,0) | (1,0) | (1,1) | (0,0) | (0,1) |
| (1,1) | (1,1) | (1,0) | (0,1) | (0,0) |

Multiplication table for $R$

| · | (0,0) | (0,1) | (1,0) | (1,1) |
|---|---|---|---|---|
| (0,0) | (0,0) | (0,0) | (0,0) | (0,0) |
| (0,1) | (0,0) | (0,0) | (0,1) | (0,1) |
| (1,0) | (0,0) | (0,1) | (1,0) | (1,1) |
| (1,1) | (0,0) | (0,1) | (1,1) | (1,0) |

3. Let $(a,b)$ and $(c,d) \in R$

- **Commutative multiplication?**
  $(a,b) \odot (c,d) = (ac, ab+bc)$ and
  $(c,d) \odot (a,b) = (ca, cd+da)$
  With the commutative multiplication property of $\mathbb{Z}_2$ we have that $ac = ca$ and also with the commutative addition property of $\mathbb{Z}_2$ we have that $ad+bc = cb+da$ thus:
  $(ac, ad+bc) = (ca, cb+da)$
  $\therefore$ R is Commutative multiplicative. □
- **Does it have an Identity?**
  R has an identity if $(a,b) \odot (x,y) = (a,b) \iff ax = a and ay + bx = b$ so we

have that $x = 1_{\mathbb{Z}_2} = 1$ and $y = 0_{\mathbb{Z}_2} = 0$
$\therefore$ R has an identity, $1_R = (1, 0)$. $\square$

- **Integral Domain?**
  R is commutative ring with identity $1_R \neq 0_R$
  and $(a, b) \odot (x, y) = (0, 0) \iff ax = 0$ and $ay + bx = 0$ **if**

  - $(a \neq 0$ and $b \neq 0)$
    $ax = 0 \to x = 0 \to bx = 0 \to ay + bx = 0 \iff ay + 0 = 0 \iff y = 0$
    **then**
    $(x, y) = (0, 0)$
    **or**
  - $(x \neq 0$ and $y \neq 0)$
    $ax = 0 \to a = 0 \to ay = 0 \to ay + bx = 0 \iff 0 + bx = 0 \iff b = 0$
    **then**
    $(a, b) = (0, 0)$

  $\therefore$ R is an integral domain. $\square$
- **Is is a field?**
  R is commutative ring with identity $1_R \neq 0_R$
  and for each $(a, b) \neq 0_R$ we have that $(a, b) \odot (x, y) = (1, 0) \iff ax = 1$,
  but if $a = 0$ there is no $x \in R$ that give $ax = 1$
  $\therefore R$ is not a field $\times$

4. Let $(a, 0), (b, 0) \in S$

   - **Closed under addition?**
     Since $a + b \in \mathbb{Z}_2 \to (a, 0) \oplus (b, 0) = (a + b, 0 + 0) = (a + b, 0) \in S$ ✓
   - **Closed under multiplication?**
     Since $ab \in \mathbb{Z}_2 \to (a, 0) \odot (b, 0) = (ab, 0 \cdot 0) = (ab, 0) \in S$ ✓
   - $0_R \in R$**?**
     Since $0 \in \mathbb{Z}_2 \to 0_R = (0, 0) \in S$ ✓
   - **Closed under subtraction*?**
     If $(a, 0) \oplus (x, y) = (0, 0) \iff a + x = 0 and 0 + y = 0$
     $a + x = 0 \iff x = -a = a \in \mathbb{Z}_2$
     $0 + y = 0 \iff y = 0$
     $\therefore (x, y) = (0, 0) \in S$ ✓

5. - $R \cong \mathbb{Z}_2 \times \mathbb{Z}_2$**?**
     Assume there is a ring homomorphsim function/mapping $f : R \to \mathbb{Z}_2 \times \mathbb{Z}_2$
     Then given $(a, b), (c, d) \in R$ we can see that $f((a, b) \oplus (c, d)) = f((a, b)) + f((c, d))$ since $\oplus$ is the same for $R$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$
     However, $f((a, b) \odot (c, d)) \neq f((a, b)) \cdot f((c, d))$ No matter the mapping, it will not be ring homomorphsim.
     $\therefore R$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ $\times$

- **$R \cong \mathbb{Z}_4$?**
  Assume there is a ring homomorphsim function/mapping $g : R \to \mathbb{Z}_4$ Then $(0,0) \leftrightarrow [0]$ (by theorem 3.10). Then by choosing
  $(1,0) \leftrightarrow [1]$
  $(0,1) \leftrightarrow [2]$
  $(1,1) \leftrightarrow [3]$
  we can see that $g((a,b) \oplus (c,d)) = g((a,b)) + g((c,d))$ However, $g((a,b) \odot (c,d)) \neq g((a,b)) \cdot g((c,d))$ No matter the mapping, it will not be ring homomorphsim.

  Addition table for $\mathbb{Z}_4$

  | + | [0] | [1] | [2] | [3] |
  |---|---|---|---|---|
  | [0] | [0] | [1] | [2] | [3] |
  | [1] | [1] | [2] | [3] | [0] |
  | [2] | [2] | [3] | [0] | [1] |
  | [3] | [3] | [0] | [1] | [2] |

  Multiplication table for $\mathbb{Z}_4$

  | · | [0] | [1] | [2] | [3] |
  |---|---|---|---|---|
  | [0] | [0] | [0] | [0] | [0] |
  | [1] | [0] | [1] | [2] | [3] |
  | [2] | [0] | [2] | [0] | [2] |
  | [3] | [0] | [3] | [2] | [1] |

  $\therefore R$ is not isomorphic to $\mathbb{Z}_4$ $\times$

6. Since $\mathbb{Z}_2[x]$ is a polynomial with coefficients in a commutative ring $\mathbb{Z}_2$ with identity, it follows by definition that $\mathbb{Z}_2$ is a commutative ring with identity.

   - **Homomorphic?**

     - $\varphi(\sum a_i X^i + \sum b_i X^i)$
       $= \varphi(\sum (a_i + b_i) X^i)$
       $= ((a_0 + b_0), (a_1 + b_1))$
       $= (a_0, a_1) \oplus (b_0, b_1)$
       $= \varphi(\sum a_i X^i) \oplus \varphi(\sum b_i X^i)$ ✓
     - $\varphi(\sum a_i X^i \times \sum b_i X^i)$
       $= \varphi(\sum c_i X^i)$ where $c_i = \sum_{n=0}^{i} a_i b_{i-n}$ where $n = 1$ because $\mathbb{Z}_2$ has to elements
       $= (c_0, c_1)$, where $c_0 = a_0 b_0$ and $c_1 = a_0 b_1 + a_1 b_0$
       $= (a_0 b_0, a_0 b_1 + a_1 b_0)$
       $= (a_0, a_1) \odot (b_0, b_1)$
       $\varphi(\sum a_i X^i) \odot \varphi(\sum b_i X^i)$ ✓

     $\therefore \varphi$ is homomorphic. □

- **Injective?**
assume $\varphi$ is injective then
$\varphi(\sum a_i X^i) = \varphi(\sum b_i X^i)$
$\iff (a_0, a_1) = (b_0, b_1)$
$\iff a_0 = b_0$ and $a_1 = b_1$
$\iff (\sum a_i X^i) = (\sum b_i X^i)$
$\therefore \varphi$ is injective. $\square$

- **Surjetive?**
assume $(a_0, a_1) \in R$ and that $\varphi$ is surjective then there exists $\sum b_i X^i \in \mathbb{Z}_2[x]$ such that $\varphi(\sum b_i X^i) = (a_0, a_1) \iff (b_0, b_1) = (a_0, a_1) \iff b_0 = a_0$ and $b_1 = a_1$
$\therefore \varphi$ is surjective $\square$

7. Since $\mathbb{Z}_7[x]$ is a field we can use the division algorithm(Theorem 4.6) on it.

$$x^4 - 2x + 1 = (2x^2 + 1) * (4x^2 + 5) + (5x + 3) \text{ in } \mathbb{Z}_7[x]$$

8. 
   - $P :=$ **Polynomials of degree less than 5**
     - If for all $a, b \in R[x], ab = 0$ then it follows that $P$ will be closed under multiplication.
     - The zero polynomial will be in this subset by the definition of the subset.
     - $deg(f(x) + g(x)) \leq max\{deg(f(x)), deg(g(x)\}$ for $f(x), g(x) \in$ this subset
     - Same for subtraction

     ✓

     - However, if $ab \neq 0$, it will not be closed under multiplication because, eg. $x^4 \cdot x^4 = x^8$ with $deg > 5$. Therefore will this subset not be a subring of $R[x]$.

     ×

   - $O :=$ **Polynomials in which the odd powers of X have coefficient 0**
     - The zero polynomial has all the coefficients $0_R$, therefore it is in $O$.
     - if $f(x) = \sum a_i X^i, g(x) = \sum b_i X^i \in O$ then so is $f(x) - g(x) \iff \sum a_i X^i - \sum b_i X^i = \sum (a_i - b_i) X^i \in O$, because odd $i$ we have that $a_i = 0$ and $b_i = 0$ thus $a_i - b_i = 0$.
     - closed under addition since, given $f(x) = \sum a_i X^i, g(x) = \sum b_i X^i \in O$, $f(x) + g(x) \iff \sum a_i X^i + \sum b_i X^i = \sum (a_i + b_i) X^i \in O$, because for an odd $i$ we have that $a_i = 0$ and $b_i = 0$ thus $a_i + b_i = 0$.
     - closed under multiplication since, given $f(x) = \sum a_i X^i, g(x) = \sum b_i X^i \in O$, $f(x)g(x) \iff \sum a_i X^i \cdot \sum b_i X^i = \sum (a_i b_i) X^i \in O$, because for an odd $i$ we have that $a_i = 0$ and $b_i = 0$ thus $a_i b_i = 0$.

     ✓

- $E :=$ **Polynomials in which the even powers of X have coefficient 0**

  - The zero polynomial has all the coefficients $0_R$, therefore it is in $E$.
  - if $f(x) = \sum a_i X^i, g(x) = \sum b_i X^i \in O$ then so is $f(x) - g(x) \iff \sum a_i X^i - \sum b_i X^i = \sum (a_i - b_i) X^i \in O$, because odd $i$ we have that $a_i = E$ and $b_i = 0$ thus $a_i - b_i = 0$.
  - closed under addition since, given $f(x) = \sum a_i X^i, g(x) = \sum b_i X^i \in E$, $f(x) + g(x) \iff \sum a_i X^i + \sum b_i X^i = \sum (a_i + b_i) X^i \in E$, because for an even $i$ we have that $a_i = 0$ and $b_i = E$ thus $a_i + b_i = 0$.
  - If $a_i b_i = 0$ for $a, b \in R$ then $E$ is closed under multiplication.

    ✓
  - However, if $a_i b_i \neq 0 \in R$ then $E$ is not closed under multiplication, because given $f(x) = \sum a_i X^i, g(x) = \sum b_i X^i \in E$ for an odd $i$, $f(x)g(x) \iff \sum a_i X^i \cdot \sum b_i X^i = \sum (a_i b_i) X^{2i} \to 2i =$ even, but $a_i b_i \neq 0$

    ×

9. (a) $f(x) = \sqrt{x}$
   $f$ is not ring homomorphsims, because
   $$f(a+b) = \sqrt{a+b} \neq f(a) + f(b) = \sqrt{a} + \sqrt{b}$$
   □

   (b) $g(x) = \sqrt{x}$
   $g$ is not ring homomorphsims, because
   $$g(a+b) = 3^{a+b} = 3^a \cdot 3^b \neq g(a) + g(b) = 3^a + 3^b$$
   □