MATH 4042 HW 1

David Chen, dc3451

January 20, 2021

Question 1

a

1. We want first that Y^+ is an abelian group under addition. First, addition is associative:

$$\begin{aligned}((n_1, a_1) + (n_2, a_2)) + (n_3, a_3) &= (n_1 + n_2, a_1 + a_2) + (n_3, a_3) \\ &= ((n_1 + n_2) + n_3, (a_1 + a_2) + a_3) \\ &= (n_1 + (n_2 + n_3), a_1 + (a_2 + a_3)) \\ &= (n_1, a_1) + ((n_2, a_2) + (n_3, a_3))\end{aligned}$$

   and commutative:

$$(n_1, a_1) + (n_2, a_2) = (n_1 + n_2, a_1 + a_2) = (n_2 + n_1, a_2 + a_1) = (n_2, a_2) + (n_1, a_1)$$

   with identity $(0, 0)$ (where the latter 0 is the additive identity in Y)

$$(n, a) + (0, 0) = (n + 0, a + 0) = (n, a)$$

   and inverses:

$$(n, a) + (-n, -a) = (n - n, a - a) = (0, 0)$$

2. Second, we have that multiplication is associative (note that due to the distributive property, $a_1(na_2) = a_1(a_2 + a_2 \cdots + a_2) = a_1a_2 + \ldots a_1a_2 = n(a_1a_2)$ for $n \in \mathbb{Z}$):

$$\begin{aligned}(n_1, a_1) \cdot ((n_2, a_2) \cdot (n_3, a_3)) &= (n_1, a_1) \cdot (n_2n_3, n_2a_3 + n_3a_2 + a_2a_3) \\ &= (n_1n_2n_3, n_1(n_2a_3 + n_3a_2 + a_2a_3) + n_2n_3a_1 + a_1(n_2a_3 + n_3a_2 + a_2a_3)) \\ &= (n_1n_2n_3, n_2n_3a_1 + n_1n_3a_2 + n_1n_2a_3 + n_1a_2a_3 + n_2a_1a_3 + n_3a_1a_2) \\ ((n_1, a_1) \cdot (n_2, a_2)) \cdot (n_3, a_3) &= (n_1n_2, n_1a_2 + n_2a_1 + a_1a_2) \cdot (n_3, a_3) \\ &= (n_1n_2n_3, n_1n_2a_3 + n_3(n_1a_2 + n_2a_1 + a_1a_2) + a_1a_2(n_1a_2 + n_2a_1 + a_1a_2)) \\ &= (n_1n_2n_3, n_2n_3a_1 + n_1n_3a_2 + n_1n_2a_3 + n_1a_2a_3 + n_2a_1a_3 + n_3a_1a_2)\end{aligned}$$

3. Lastly, we check distributivity:

$$\begin{aligned}(n_1, a_1) \cdot ((n_2, a_2) + (n_3, a_3)) &= (n_1, a_1) \cdot (n_2 + n_3, a_2 + a_3) \\ &= (n_1(n_2 + n_3), n_1(a_2 + a_3) + (n_2 + n_3)a_1 + a_1((a_2 + a_3))) \\ &= (n_1n_2 + n_1n_3, n_1a_2 + n_2a_1 + a_1a_2 + n_1a_3 + n_3a_1 + a_1a_3) \\ &= ((n_1, a_1) \cdot (n_2, a_2)) + ((n_1, a_1) \cdot (n_3, a_3)) \\ ((n_1, a_1) + (n_2, a_2)) \cdot (n_3, a_3)) &= (n_1 + n_2, a_1 + a_2) \cdot (n_3, a_3) \\ &= ((n_1 + n_2)n_3, (n_1 + n_2)a_3 + n_3(a_1 + a_2) + (a_1 + a_2)a_3) \\ &= (n_1n_3 + n_2n_3, n_1a_3 + n_3a_1 + a_1a_3 + n_2a_3 + n_3a_2 + a_2a_3) \\ &= ((n_1, a_1) \cdot (n_3, a_3)) + ((n_2, a_2) \cdot (n_3, a_3))\end{aligned}$$

4. To check the identity, we have

$$\begin{aligned}(n, a) \cdot (1, 0) &= (n1, n0 + 1a + a0) = (n, a) \\ (1, 0) \cdot (n, a) &= (1n, 1a + 0n + 0a) = (n, a)\end{aligned}$$

b

Note

$$(n, a) \cdot (0, 1) = (0, n \cdot 1 + a0 + a1) = (0, n + a)$$

and

$$(0, 1) \cdot (n, a) = (0, 0a + n1 + 1a) = (0, n + a)$$

where $n = 1 + 1 + \cdots + 1$ in Y.

Secondly, $(0, y_1) + (0, y_2) = (0, y_1 + y_2) \in I_Y$, $(0, y) \in I_Y \implies (0, -y) \in I_Y$, and $(0, 0) \in I_Y$, so I_Y is a subgroup under addition.

c

We already have that since an ideal is a subgroup of R (itself an abelian group with addition) under addition, it already is an abelian group under addition. Associativity follows from associativity of the multiplication of R, since for $x, y, z \in I$, associativity in R gives $x(yz) = (xy)z$ in R, but since I is an ideal, xyz also lies in I. Similarly, distributivity also comes since in R, $x(y + z) = xy + xz$, and since I an ideal, $xy, xz \in I$ and thus $xy + xz$ also lie in I; $(y + z)x = yx + zx$ also lies in I.

d

We have that for $n \in \mathbb{Z}, p \in (x)$, $\phi : (n, p) \mapsto p+n$, where on the right $n = 1+1+\cdots+1$ in $\mathbb{Z}[x]$, is a isomorphism taking $(x)^+ \to \mathbb{Z}[x]$. First, to see it is bijective, if $\phi((n_1, p_1)) = \phi((n_2, p_2))$, then we have that $p_1+n_1 = p_2+n_2$. However, since $p_1 \in (x)$, we have that $p_1 = (\sum_{i=0}^{n} a_i x^i)\, x$, and similarly for p_2. In particular, this means that p_1, p_2 have no (nonzero) terms of degree 0, and since n_1, n_2 are both terms of degree 0, we have that $n_1 = n_2$, which then immediately yields $p_1 = p_2$, so ϕ is injective. For surjectivity, any polynomial $p \in \mathbb{Z}[x]$ where $p = \sum_{i=0}^{n} a_i x^i$ has preimage $(a_0, \sum_{i=1}^{n} a_i x^i) = (a_0, (\sum_{i=1}^{n} a_i x^{i-1})x)$. Checking that it is a homomorphism,

$$\phi((n_1, p_1) + (n_2, p_2)) = \phi((n_1 + n_2, p_1 + p_2)) = p_1 + p_2 + n_1 + n_2 = \phi((n_1, p_1)) + \phi((n_2, p_2))$$

since addition commutes.

$$\begin{aligned}\phi((n_1, p_1) \cdot (n_2, p_2)) &= \phi((n_1 n_2, n_1 p_2 + n_2 p_1 + p_1 p_2)) \\ &= p_1 p_2 + n_1 p_2 + n_2 p_1 + n_1 n_2 \\ &= (p_1 + n_1)(p_2 + n_2) \\ &= \phi((n_1, p_1))\phi((n_2, p_2))\end{aligned}$$

and lastly,

$$\phi((1, 0)) = 0 + 1 = 1$$

so ϕ is a homomorphism.

Question 2

a

1. Checking that this forms an abelian group under addition, we have that

   $$(a_1, a_2) + (b_1, b_2) = (a_1 + a_2, b_1 + b_2) = (a_2 + a_1, b_2 + b_1) = (a_2, b_2) + (a_1, b_1)$$

   for commutativity and

   $$\begin{aligned}(a_1, a_2) + ((b_1, b_2) + (c_1, c_2)) &= (a_1, a_2) + (b_1 + c_1, b_2 + c_2) \\ &= (a_1 + b_1 + c_1, a_2 + b_2 + c_2) \\ &= (a_1 + b_1, a_2 + b_2) + (c_1, c_2) \\ &= ((a_1, a_2) + (b_1, b_2)) + (c_1, c_2)\end{aligned}$$

   for associativity, with identity $(0, 0)$ (the zero element in the ring)

   $$(a_1, a_2) + (0, 0) = (a_1, a_2)$$

   and inverses:

   $$(a_1, a_2) + (-a_1, -a_2) = (0, 0)$$

2. Checking that multiplication is associative,

$$\begin{aligned}(a_1, a_2)((b_1, b_2)(c_1, c_2)) &= (a_1, a_2)(b_1c_1, b_2, c_2)\\ &= (a_1b_1c_1, a_2b_2c_2)\\ &= (a_1b_1, a_2b_2)(c_1, c_2)\\ &= ((a_1, a_2)(b_1, b_2))(c_1, c_2)\end{aligned}$$

3. Checking distributivity,

$$\begin{aligned}(a_1, a_2)((b_1, b_2) + (c_1, c_2)) &= (a_1, a_2)(b_1 + c_1, b_2 + c_2)\\ &= (a_1(b_1 + c_1), a_2(b_2 + c_2))\\ &= (a_1b_1 + a_1c_1, a_2b_2 + a_2c_2)\\ &= (a_1b_1, a_2b_2) + (a_1c_1, a_2c_2)\\ &= (a_1, a_2)(b_1, b_2) + (a_1, a_2)(c_1, c_2)\\ ((b_1, b_2) + (c_1, c_2))(a_1, a_2) &= (b_1 + c_1, b_2 + c_2)(a_1, a_2)\\ &= ((b_1 + c_1)a_1, (b_2 + c_2)a_2)\\ &= (b_1a_1 + c_1a_1, b_2a_2 + c_2a_2)\\ &= (b_1a_1, b_2a_2) + (c_1a_1, c_2a_2)\\ &= (b_1, b_2)(a_1, a_2) + (c_1, c_2)(a_1, a_2)\end{aligned}$$

4. Checking the identity to be $(1, 1)$, we have

$$(a_1, a_2) \cdot (1, 1) = (a_1, a_2)$$

and

$$(1, 1) \cdot (a_1, a_2) = (a_1, a_2)$$

b

To check that $I_1 \times I_2$ is a subgroup, we have that $0 \in I_1, I_2 \implies (0, 0) \in I_1 \times I_2$, and also that $(a_1, a_2), (b_1, b_2) \in I_1 \times I_2 \implies (a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \in I_1 \times I_2$, and $(a, b) \in I_1 \times I_2 \implies (-a, -b) \in I_1 \times I_2$, so we have the identity, closure and inverses.
For multiplication, we get for $(r_1, r_2) \in R$, and $(a_1, a_2) \in I_1 \times I_2$,

$$(r_1, r_2)(a_1, a_2) = (r_1a_1, r_2a_2)$$

and since a_1, a_2 are members of ideals themselves, the product is in $I_1 \times I_2$. Similarly,

$$(a_1, a_2)(r_1, r_2) = (a_1r_1, a_2r_2) \in I_1 \times I_2$$

c

Consider any ideal $I \in R_1 \times R_2$ and the corresponding sets $I_1 = \{a \mid \exists(a, \cdot) \in I\}$ and $I_2 = \{b \mid \exists(\cdot, b) \in I\}$. Then, we want that $I = I_1 \times I_2$.

Firstly, we have that $(a, b) \in I$ clearly implies $(a, b) \in I_1 \times I_2$ by definition. Then, if we have some $(a, b) \in I_1 \times I_2$, then there is some $(a, b') \in I$ and some $(a', b) \in I$ as well. Then, $(1, b)(a, b') = (a, bb') \in I$, and $(a', b)(1, b') = (a', bb') \in I$, and thus $(a, bb') - (a', bb') + (a', b) = (a, b) \in I$.

The last thing to show is that both I_1, I_2 are ideals. In particular, there is nothing significant about the first position, so showing it for I_1 is the same as for I_2. Then, picking any $r_1 \in R_1$ and $a \in I_1$, we have that there is some $(a, b) \in I$ and $(r_1, 1)(a, b) = (r_1 a, b) \in I \implies r_1 a \in I$ and similarly $(a, b)(r_1, 1) = (ar_1, b) \in I \implies ar_1 \in I$. Furthermore, I contains the identity, since $(0, 0) \in I \implies 0 \in I_1$, $a \in I_1 \implies (a, b) \in I \implies (-a, -b) \in I \implies -a \in I_1$ and $a_1, a_2 \in I \implies (a_1, b_1), (a_2, b_2) \in I \implies (a_1 + a_2, b_1 + b_2) \in I \implies a_1 + a_2 \in I$ and we have closure, the identity, and inverses.

d

I'm not sure why this problem is given as an isomorphism; these sets are (should be?) identical, which does give us a trivial isomorphism in the identity. If we have some $(r_1, r_2) \in (R_1 \times R_2)^\times$, then $\exists(r_1', r_2')$ such that $(r_1, r_2)(r_1', r_2') = (1, 1) \implies r_1 r_1' = 1$ and $r_2 r_2' = 1$, so $r_1 \in R_1^\times$ and $r_2 \in R_2^\times$, and so $(R_1 \times R_2)^\times \subseteq R_1^\times \times R_2^\times$. Then, if we have some $r_1 \in R_1^\times$ and $r_2 \in R_2^\times$, there are r_1^{-1}, r_2^{-1} units such that $r_1 r_1^{-1} = 1$ and $r_2 r_2^{-1} = 1$, so we have that $(r_1, r_2)(r_1^{-1}, r_2^{-1}) = (1, 1) \implies (r_1, r_2) \in (R_1 \times R_2)^\times$, so $R_1^\times \times R_2^\times \subseteq (R_1 \times R_2)^\times$, so the two groups are equal.

Question 3

Take $\phi : n \mapsto (n \bmod 2, n \bmod 3)$ (so for example $\phi(4) = (0, 1)$). That this is a bijection is immediate from the Chinese Remainder Theorem (since these are isomorphic as groups) but we can also check this directly:

$$\begin{aligned}
\phi(0) &= (0, 0) \\
\phi(1) &= (1, 1) \\
\phi(2) &= (0, 2) \\
\phi(3) &= (1, 0) \\
\phi(4) &= (0, 1) \\
\phi(5) &= (1, 2)
\end{aligned}$$

so we have that ϕ is bijective (and sends $1 \mapsto (1,1)$). That it is a ring homomorphism follows immediately from basic properties of modular arithmetic:

$$\phi(a+b) = (a+b \bmod 2, a+b \bmod 3) = (a \bmod 2, a \bmod 3)+(b \bmod 2, b \bmod 3) = \phi(a)+\phi(b)$$

$$\phi(ab) = (ab \bmod 2, ab \bmod 3) = (a \bmod 2, a \bmod 3) \cdot (b \bmod 2, b \bmod 3) = \phi(a)\phi(b)$$

Question 4

a

$$(1-e)^2 = 1^2 - e1 - 1e + e^2 = 1 - 2e + e = 1 - e$$

b

Consider

$$e(1-e) = e - e^2 = e - e = 0$$

but if $e \neq 0, 1$, we have that $e \neq 0$ and $1 - e \neq 0$, so this is not an integral domain.

c

Consider $(0,1) \in R_1 \times R_2$ which is neither the zero element $(0,0)$ nor the multiplicative identity $(1,1)$. Then, we have that $(0,1)^2 = (0,1)$, so this (as well as $(1,0)$) is the element we are looking for.

d

Suppose that $(a+bi)(c+di) = 0$, such that $ac - bd + (ad+bc)i = 0$ and in particular $ad + bc = 0$; note that this also yields

$$(a-bi)(c-di) = ac - bd - (ad+bc)i = 0$$

so

$$(a+bi)(c+di)(a-bi)(c-di) = (a^2+b^2)(c^2+d^2) = 0$$

for $a, b, c, d \in \mathbb{Z}$. Then, one of a^2+b^2 and c^2+d^2 must vanish, and since $a^2, b^2, c^2, d^2 > 0$ for nonzero a, b, c, d, we have one of the pairs a, b and c, d must vanish, so one of $a+bi$ and $c+di$ must be 0. Thus, $\mathbb{Z}[i]$ must be an integral domain.

Question 5

a

Again, ideals are (from class) subgroups under addition in the ring that they live it, so it already satisfies that it is an abelian group under addition. Then, we still have for $x, y, z \in (e)$, the property that ideals absorb multiplication (and associativity in R) gives $x(yz) = (xy)z$ and that $xyz \in (e)$ as well; similarly, distributivity in R again gives that $x(y+z) = xy + xz$ and $(y+z)x = yx + zx$, and that both are in (e). Note that (e) does not contain 1; however, we do have that for any element $re \in (e)$, $e(re) = (re)e = re^2 = re$, so e serves as the identity in (e).

b

We can show that $R \cong (e) \times (1-e)$. In particular, the first part, since it is indenpendent of the choice of idempotent, shows that both (e) and $(1-e)$ are rings (with identities e and $1-e$ respectively). Then, consider the mapping $\phi : a \mapsto (ae, a(1-e))$, such that

$$\phi(a+b) = ((a+b)e, (a+b)(1-e)) = (ae+be, a(1-e)+b(1-e)) = (ae, a(1-e))+(be, b(1-e)) = \phi(a)+\phi(b)$$

$$\phi(ab) = ((ab)e, (ab)(1-e)) = (abe^2, ab(1-e)^2) = (ae, a(1-e)) \cdot (be, b(1-e)) = \phi(a)\phi(b)$$

$$\phi(1) = (e, (1-e))$$

which is the identity in $(e) \times (1-e)$ since we showed earlier the identity in those rings were e and $1-e$ respectively.

In particular, this is surjective, since if we have some $re \in (e)$, $s(1-e) \in (1-e)$, then we get that

$$\phi(re+s(1-e)) = ((re+s(1-e))e, (re+s(1-e))(1-e)) = (re^2+s(1-e)e, re(1-e)+s(1-e)^2) = (re, s(1-e))$$

so we have a preimage for every element in $(e) \times (1-e)$. Then, for injectivity, we can check the kernel of ϕ to be trivial: if $(ae, a(1-e)) = 0$, then $-ae = a(1-e) = 0 \implies a = 0$.

Question 6

For this problem, if we have some matrix A, let the entry in the i^{th} row and j^{th} column as A_{ij}.

a

First, we need that $M_n(I)$ is a subgroup under addition; this is clear since matrix addition is just component-wise, so we have that $0 \in I \implies 0 \in M_n(I)$, $A \in M_n(I) \implies A_{ij} \in I \implies$

$-A_{ij} \in I \implies -A \in M_n(I)$, and $A, B \in M_n(I) \implies A_{ij}, B_{ij} \in I \implies A_{ij} + B_{ij} \in I \implies A + B \in M_n(I)$ so we get the identity, inverses, and closure.

Further, we have for $A \in M_n(I)$, $B \in M_n(R)$, each entry satisfies

$$(AB)_{ij} = \sum_{k=1}^{n} A_{i,k} B_{k,j}$$

but since $A_{i,k} \in I$, $A_{i,k}B_{k,j} \in I$ as well, so we get that $(AB)_{ij} \in I$ and so $AB \in M_n(I)$. Similarly,

$$(BA)_{ij} = \sum_{k=1}^{n} B_{i,k} A_{k,j}$$

so $A_{k,j} \in I \implies B_{i,k}A_{k,j} \in I \implies (BA)_{ij} \in M_n(I) \implies BA \in M_n(I)$.

b

For this part, denote the matrix

$$\begin{bmatrix} 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{bmatrix}$$

where the 1 is is in the i^{th} row and j^{th} column as E_{ij}.

We can show that $S = \{A_{11} \mid A \in I_n\}$ (for some ideal I_n of $M_n(R)$) is an ideal of R, and that $I_n = M_n(S)$. First, to see that it is an ideal, we can consider for any element $r \in R$ and element $a \in S$ the matrix $rE_{11} \in M_n(R)$ and the matrix $sE_{11} \in I_n$, such that since I_n is an ideal, $(rE_{11})(sE_{11}) = rsE_{11}^2 = rsE_{11}$ and $(sE_{11})(rE_{11}) = srE_{11}$ are both in I_n, and thus $rs, sr \in S$. That S is a subgroup under addition is easy, since we get that $0 \in I_n \implies 0 \in S$, $a, b \in S \implies aE_{11} + bE_{11} = (a+b)E_{11} \implies a + b \in S$, and $a \in S \implies -aE_{11} \in I_n \implies -a \in S$, so we get the identity, closure, and inverses.

To see that $I_n = M_n(S)$, consider $A \in I_n$ and any entry A_{ij}. Then, we can consider the product P_iAP_j, where P_k is the permutation matrix corresponding to the permutation $(1, k)$ (that is, the identity matrix with the first row and the k^{th} row swapped). Then, we have that this is contained in the ideal, and $(P_iAP_j)_{11} = A_{ij}$, so $A_{ij} \in S$, so S contains all of the entries of I_n, but by definition S is a subset of the entries of I_n, so I_n has coefficients exactly in S, giving $I_n \subseteq M_n(S)$. Then, consider that for any $A \in M_n(S)$, we can write $A = \sum_{i=1}^{n} \sum_{j=1}^{n} A_{ij}E_{ij}$, but each $A_{ij}E_{ij} \in I_n$, so we get that $A \in I_n$, so $M_n(S) \subseteq I_n$ as well, so finally $I_n = M_n(S)$.