Chris Hayduk
Math A4900
Homework 9
11/13/2020

1. **Rings.**

(a) The *center* of a ring R is $Z(R) = \{z \in R \mid zr = rz \text{ for all } r \in R\}$ (i.e. the center of the underlying multiplicative semigroup).

(i) Show that $Z(R)$ is a subring of R containing 0 and 1 (if it exists).

Proof. We know $Z(R) \subset R$ by definition by the set. In addition, we have that $Z(R) \neq \varnothing$ because $0r = 0 = r0$ for all $r \in R$. Hence, $0 \in Z(R)$. Moreover, if 1 exists, then $1r = r = r1$ for all $r \in R$, so $1 \in Z(R)$ as well. Now fix $a, b \in Z(R)$. Then $ar = ra$ and $br = rb$ for all $r \in R$. Hence,

$$\begin{aligned}(a-b)r &= ar - br \\ &= ra - rb \\ &= r(a-b)\end{aligned}$$

for all $r \in R$. Thus, $a - b \in Z(R)$ as well, and so $Z(R)$ is closed under addition. Now, we will check multiplication,

$$\begin{aligned}(ab)r &= a(br) \\ &= a(rb) \\ &= (ar)b \\ &= (ra)b \\ &= r(ab)\end{aligned}$$

So for all $r \in R$, we have $(ab)r = r(ab)$. Hence, $ab \in Z(R)$ and $Z(R)$ is closed under multiplication. Thus, $Z(R)$ is a subring of R ☐

(ii) Is $Z(R)$ necessarily an ideal of R?

Proof. Recall that $Z(R)$ is an ideal of R if

$$rZ(R), Z(R)r \subset Z(R)$$

for every $r \in R$.

Let $r \in R$ such that there exists $r' \in R$ which r does not commute with. That is, $r \notin Z(R)$. If such an r exists, then consider $rZ(R)$. Fix $a \in Z(R)$ and consider ra. We have that $r'(ra) \neq (ra)r'$ because r and r' do not commute. Hence, $ra \notin Z(R)$ and so $rZ(R) \not\subset Z(R)$. Thus, $Z(R)$ is not necessarily an ideal of R.

$Z(R)$ is an ideal of R if $Z(R) = \{0\}$ (i.e. the only element that commutes with everything in R is 0) or $Z(R) = R$ (i.e. R is a commutative ring). ☐

(iii) Show that the center of a division ring is a field.

Proof. Recall that division ring R is a ring with identity 1, where $1 \neq 0$, and with the property that every nonzero element $a \in R$ has a multiplicative inverse, i.e. there exists $b \in R$ such that $ab = ba = 1$. Since every element commutes with its inverse, we have that $Z(R)$ is closed under multiplication, subtraction, and inverses.

Now recall $Z(R)$ is a field if $(Z(R), +)$ is an abelian group and $(Z(R) - \{0\}, \cdot)$ is also an abelian group, and the following distributive law holds:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

for all $a, b, c \in Z(R)$.

We have that $(Z(R), +)$ is an abelian group based on the definition of rings and the fact that $Z(R)$ is a subring of R. Now consider $(Z(R) - \{0\}, \cdot)$. From properties of rings, we know that $\cdot$ is a well-defined operation and that is is associative. Hence, we just need to check that $(Z(R) - \{0\}, \cdot)$ has an identity element and is closed under inverses in order to show that it is a group.

In part (i), we proved that if 1 exists, we have that $1 \in Z(R)$. Hence, $1 \in Z(R) - \{0\}$. □

(b) Decide which of the following are ideals in $\mathbb{Z} \times \mathbb{Z}$:

$$\{(a, a) \mid a \in \mathbb{Z}\}, \qquad \{(a, -a) \mid a \in \mathbb{Z}\}, \qquad \{(2a, 0) \mid a \in \mathbb{Z}\}.$$

Proof. $\{(a, a) \mid a \in \mathbb{Z}\}$ is not an ideal in $\mathbb{Z} \times \mathbb{Z}$ because $(2, 3) \in \mathbb{Z} \times \mathbb{Z}$ and $(1, 1) \in \{(a, a) \mid a \in \mathbb{Z}\}$ but $(2, 3) \cdot (1, 1) = (2, 3) \notin \{(a, a) \mid a \in \mathbb{Z}\}$. Hence,

$$(2, 3) \cdot \{(a, a) \mid a \in \mathbb{Z}\} \not\subset \{(a, a) \mid a \in \mathbb{Z}\}$$

$\{(a, -a) \mid a \in \mathbb{Z}\}$ is also not an ideal in $\mathbb{Z} \times \mathbb{Z}$ because $(2, 3) \in \mathbb{Z} \times \mathbb{Z}$ and $(1, -1) \in \{(a, -a) \mid a \in \mathbb{Z}\}$ but $(2, 3) \cdot (1, -1) = (2, -3) \notin \{(a, -a) \mid a \in \mathbb{Z}\}$. Hence,

$$(2, 3) \cdot \{(a, -a) \mid a \in \mathbb{Z}\} \not\subset \{(a, -a) \mid a \in \mathbb{Z}\}$$

$\{(2a, 0 \mid a \in \mathbb{Z}\}$ is an ideal in $\mathbb{Z} \times \mathbb{Z}$. Fix $(b_1, b_2) \in \mathbb{Z} \times \mathbb{Z}$ and fix $(2a, 0) \in \{(2a, 0 \mid a \in \mathbb{Z}\}$. Then we have,

$$\begin{aligned} (b_1, b_2) \cdot (2a, 0) &= (b_1 \cdot 2a, b_2 \cdot 0) \\ &= (2(b_1 a), 0) \end{aligned}$$

We are able to make the last change because multiplication in $\mathbb{Z}$ is commutative. In addition, since b_1, a in $\mathbb{Z}$ and $\mathbb{Z}$ is closed under multiplication, we have that $b_1 a \in \mathbb{Z}$ as well. Hence, $(2(b_1 a), 0) \in \{(2a, 0 \mid a \in \mathbb{Z}\}$. Since $b_1, b_2, a \in \mathbb{Z}$ were chosen to be arbitrary in $\mathbb{Z}$, we have that $\{(2a, 0 \mid a \in \mathbb{Z}\}$ is a left ideal of $\mathbb{Z} \times \mathbb{Z}$.

Now fix $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$. Then we have,

$$\begin{aligned} (a, b) \cdot (c, d) &= (a \cdot c, b \cdot d) \\ &= (c \cdot a, d \cdot b) \\ &= (c, d) \cdot (a, b) \end{aligned}$$

by the commutativity of multiplication in $\mathbb{Z}$. Hence, $\mathbb{Z} \times \mathbb{Z}$ is a commutative ring and we have that the notions of left ideals and right ideals are the same. As a result, we have shown that $\{(2a, 0 \mid a \in \mathbb{Z}\}$ is closed under left and right multiplication by elements from $\mathbb{Z} \times \mathbb{Z}$, and hence $\{(2a, 0 \mid a \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z} \times \mathbb{Z}$. □

2. **Nilpotent elements.** We call an element $x \in R$ *nilpotent* if $x^n = 0$ for some $n \in \mathbb{Z}_{>0}$.

(a) Explain why the only nilpotent element of any integral domain is 0.

Proof. Recall that an integral domain is a commutative ring with identity $1 \neq 0$ and no zero divisors. That is, there are no nonzero elements a, b in R such that $ab = 0$ (so at least one of a or b must be 0).

Now let $x \in R$ and suppose x is nilpotent. That is, $x^n = 0$ for some $n \in \mathbb{Z}_{>0}$. Since R is closed under multiplication, we have $x^{n-1} \in R$. Moreover,

$$\begin{aligned} x \cdot x^{n-1} &= x^n \\ &= 0 \end{aligned}$$

However, this implies that x is a 0 divisor in R since $x \cdot x^{n-1} = 0$. But since R is an integral domain, we know that either x^{n-1} or x is 0. If $x = 0$ we are done, so let us assume that $x \neq 0$. Thus, by the fact that R is an integral domain, we have $x^{n-1} = 0$. Since n was arbitrary, this holds for any $n \in \mathbb{Z}_{>0}$. Thus, by induction we have,

$$x^2 = x \cdot x = 0$$

And hence, $x = 0$. Thus, 0 is the only nilpotent element in an integral domain. $\square$

(b) Prove that if R is commutative, then the *nilradical*, defined by

$$\mathfrak{N}(R) = \{x \in R \mid x \text{ is nilpotent }\},$$

is an ideal of R. [You may use the Binomial Theorem given in Exercise 7.3.25 without proof to show closure under addition or subtraction.]

Proof. Let $x, y \in \mathfrak{N}(R)$. Then $x^n = y^m = 0$ for some n, m. We need to show that $(x-y)^\ell = 0$ for some ℓ in order to show that $\mathfrak{N}(R)$ is closed under subtraction. Let us reformulate this as $(x + (-y))^\ell$ and apply the Binomial Theorem from Exercise 7.3.25,

$$(x + (-y))^\ell = \sum_{k=0}^{\ell} \binom{\ell}{k} x^k (-y)^{\ell-k}$$

$\square$

(c) Prove that if R is commutative, then the only nilpotent element of $R/\mathfrak{N}(R)$ is 0. Conclude that $\mathfrak{N}(R/\mathfrak{N}(R)) = 0$. [Namely, modding out by the nilradical removes all nilpotent elements.]

Proof. Let $r \in R$ and suppose,

$$\begin{aligned} \bar{0} &= \bar{r}^\ell \\ &= (r + \mathfrak{N}(R))^\ell \\ &= r^\ell + \mathfrak{N}(R) \end{aligned}$$

for some $\ell \in \mathbb{Z}_{>0}$.

Since $0 + \mathfrak{N}(R) = r^\ell + \mathfrak{N}(R)$, we have that $r^\ell \in \mathfrak{N}(R)$. Hence, there exists $n \in \mathbb{Z}_{>0}$ such that $(r^\ell)^n = r^{\ell n} = 0$. Since $\ell, n \in \mathbb{Z}_{>0}$, we have that $\ell n \in \mathbb{Z}_{>0}$. Thus, r is nilpotent and hence is in $\mathfrak{N}(R)$. As a result, $\bar{r} = \bar{0}$ and the only nilpotent element of $\mathfrak{N}(R/\mathfrak{N}(R))$ is $\bar{0}$. $\square$

(d) Show that, in $M_2(\mathbb{R})$,

$$x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

are both nilpotent, but $x + y$ is not. Conclude that the nilradical $\mathfrak{N}(R)$ is not necessarily an ideal if R is not commutative.

Proof. We have,

$$\begin{aligned} x^2 &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

and,

$$\begin{aligned} y^2 &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

Hence, both x and y are nilpotent. Now let us consider,

$$x + y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Now we will check the powers of $x + y$ to see if $(x + y)^n = 0$ for any $n \in \mathbb{Z}_{>0}$,

$$\begin{aligned} (x + y)^2 &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= I_2 \end{aligned}$$

and so,

$$\begin{aligned} (x + y)^3 &= (x + y) \cdot (x + y)^2 \\ &= (x + y) \cdot I_2 \\ &= x + y \end{aligned}$$

$$\begin{aligned} (x + y)^4 &= (x + y) \cdot (x + y)^3 \\ &= (x + y) \cdot (x + y) \\ &= I_2 \end{aligned}$$

Hence, $(x + y)^n = x + y, I_2$ for any $n \in \mathbb{Z}_{n>0}$. Thus, $x + y$ is not nilpotent. □

3. **Homomorphisms.**

(a) Show that $2\mathbb{Z}$ and $3\mathbb{Z}$ are isomorphic as groups but not as rings. [Hint: Note that any ring homomorphism has to also be an additive group homomorphism. So the additive generators of $2\mathbb{Z}$ have to map to additive generators of $3\mathbb{Z}$.]

Proof. Define $\varphi : 2\mathbb{Z} \to 3\mathbb{Z}$ by $x \mapsto 3/2 \cdot x$. Now fix $a, b \in 2\mathbb{Z}$. We have,

$$\begin{aligned} \varphi(a+b) &= 3/2 \cdot (a+b) \\ &= 3/2 \cdot a + 3/2 \cdot b \\ &= \varphi(a) + \varphi(b) \end{aligned}$$

As a result, we have that φ is a group homomorphism on the additive groups. Now let $b \in 3\mathbb{Z}$. Then $b = 3x$ for some $x \in 3\mathbb{Z}$. Let $a = 2/3 \cdot b = 2/3 \cdot 3x = 2x$. Then $a \in 2\mathbb{Z}$ and we have $\varphi(a) = 3/2 \cdot a = 3/2 \cdot 2/3b = b$. Hence, φ is surjective.

Now fix $a_1, a_2 \in 2\mathbb{Z}$ and assume $\varphi(a_1) = \varphi(a_2)$. Then we have,

$$\begin{aligned} 3/2 \cdot a_1 &= 3/2 \cdot a_2 \\ \implies a_1 &= a_2 \end{aligned}$$

Thus, φ is also injective and hence is a bijection. As a result, we have that φ is an isomorphism of the additive groups. However, note now that,

$$\begin{aligned} \varphi(ab) &= 3/2(ab) \\ &\neq (3/2)^2 ab \\ &= \varphi(a) \cdot \varphi(b) \end{aligned}$$

Hence, φ is not a ring isomorphism. □

(b) Let R be the set of (weakly) upper-triangular matrices in $M_2(\mathbb{Z})$. Prove that

$$\varphi : R \to \mathbb{Z} \times \mathbb{Z} \quad \text{defined by} \quad \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto (a, d)$$

is a surjective homomorphism and calculate its kernel.

Proof. Fix $a, b \in R$ with,

$$a = \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}$$

and,

$$b = \begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix}$$

Then, we have,

$$a + b = \begin{pmatrix} a_1 + b_1 & a_2 + b_2 \\ 0 & a_3 + b_3 \end{pmatrix}$$

and,

$$ab = \begin{pmatrix} a_1 b_1 & a_1 b_2 + a_2 b_3 \\ 0 & a_3 b_3 \end{pmatrix}$$

Now we will check the additive homomorphism property,

$$\begin{aligned} \varphi(a+b) &= (a_1 + b_1, a_3 + b_3) \\ &= (a_1, a_3) + (b_1, b_3) \\ &= \varphi(a) + \varphi(b) \end{aligned}$$

And the multiplication property,

$$\begin{aligned}\varphi(ab) &= (a_1b_1, a_3b_3) \\ &= (a_1, a_3) \cdot (b_1, b_3) \\ &= \varphi(a) \cdot \varphi(b)\end{aligned}$$

Now let $(a, d) \in \mathbb{Z} \times \mathbb{Z}$ and define $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ where $a, b, d \in \mathbb{Z}$. Then $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in R$ and

$$\varphi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = (a, d)$$

Hence, φ is surjective. Now we need to find the kernel of φ, which is the set of elements that map to $(0, 0) \in \mathbb{Z} \times \mathbb{Z}$. Note that, in the general matrix,

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

we must have $a, d = 0$ in order for $\varphi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = (0, 0)$. Thus,

$$\ker(\varphi) = \left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{Z}\right\}$$

□

(c) Let R and S be rings with identities 1_R and 1_S, respectively. Let $\varphi : R \to S$ be a non-zero ring homomorphism. Prove that if $\varphi(1_R) \neq 1_S$, then $\varphi(1_R)$ is a zero divisor in S.

Proof. Suppose $\varphi : R \to S$ is a non-zero ring homomorphism and $\varphi(1_R) \neq 1_S$. □