Question: 1

Which of the following sets are rings with respect to the usual operations of addition and multiplication? If the set is a ring, is it also a field?

a. $7\mathbb{Z}$

b. $\mathbb{Z}_{18}$

c. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$

d. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$

e. $\mathbb{Z}[\sqrt{3}\,] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$

f. $R = \{a + b\sqrt[3]{3} : a, b \in \mathbb{Q}\}$

g. $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ and } i^2 = -1\}$

h. $\mathbb{Q}(\sqrt[3]{3}\,) = \{a + b\sqrt[3]{3} + c\sqrt[3]{9} : a, b, c \in \mathbb{Q}\}$

Solution:

a. $7\mathbb{Z}$ is a ring since it is a subring of $\mathbb{Z}$. This is not hard to show. However, it lacks an identity, so it is a field.

b. $\mathbb{Z}_{18}$ is a ring because addition and mulitplcation in modulo 18 are well-defined. However, we can see that it is not a field. $2 \cdot 9 = 0$ in $\mathbb{Z}_{18}$, so we have a pair of zero divisors.

c. $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{R}$ so it is therefore a ring and a field. The fact that it is a subring is not hard to show.

d. Like the last part, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a subfield of $\mathbb{R}$ and is therfore a ring and a field.

e. $\mathbb{Z}^{\sqrt{3}}$ is a subring of $\mathbb{R}$ and is therefore a ring. Now let's analyze $\sqrt{3} \in \mathbb{Z}^{\sqrt{3}}$. Calculating the inverse of $\sqrt{3}$ gives us $\frac{1}{\sqrt{3}} \notin \mathbb{Z}^{\sqrt{3}}$. Therefore, $\mathbb{Z}^{\sqrt{3}}$ is not a field.

f. If $a = 0$ and $b = 1$, we have that $\sqrt[3]{3} \in R$. However, $\sqrt[3]{3} \cdot \sqrt[3]{3} = \sqrt[3]{9} \notin R$. Therefore, R is not closed under multiplication and is therefore not a ring.

g. $\mathbb{Z}^i$ is a field because it is a subfield of $\mathbb{C}$. By definition, it is also a ring.

h. $\mathbb{Q}(\sqrt[3]{3})$ is a subfield of $\mathbb{R}$ and is therefore a ring and a field.

Question: 12

Prove that $\mathbb{Z}[\sqrt{3}\,i] = \{a + b\sqrt{3}\,i : a, b \in \mathbb{Z}\}$ is an integral domain.

Solution: A common rule of complex numbers is that for any $z, w \in \mathbb{C}$, $|z||w| = |zw|$. Also, $\mathbb{Z}^{\sqrt{3}i} \in \mathbb{C}$, so we have that $|zw| = |z||w| \forall z, w \in \mathbb{Z}^{\sqrt{3}i}$. This means that if $z, w \neq 0$, then $|z|, |w| \neq 0$, and therefore $|z||w| = |zw| \neq 0$. So, $\mathbb{Z}^{\sqrt{3}i}$ has no zero divisors and is therefore an integral domain. 😄

Question: 24

Let R be a ring with a collection of subrings $\{R_\alpha\}$. Prove that $\bigcap R_\alpha$ is a subring of R. Give an example to show that the union of two subrings is not necessarily a subring.

Solution: Let $r, s \in \bigcap R_\alpha$. This means that $r, s \in R_\alpha$, so $rs, (r-s) \in R_\alpha$. Thus, $rs, (r-s) \in \bigcap R_\alpha$. So $\bigcap R_\alpha$ is a subring of R. 😄

An example of the union of two subrings not being a subring is how $2\mathbb{Z}$ and $3\mathbb{Z}$ are both subrings of $\mathbb{Z}$, but $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subring of $\mathbb{Z}$. We can see this because $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, but $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

Question: 30

Let R be a ring with the identity 1_R and S a subring of R with identity 1_S. Prove or disprove that $1_R = 1_S$.

Solution: I will disprove this. Let $R = \mathbb{Z}_6$ and $S = \{0, 3\}$. S is a subring of R. S is a ring because $a + b$ and ab are both in S for all four combinations of a and b. However, we know that $1_R = 1$. But in S, we can see that $3 \times 0 = 0$ and that $3 \times 3 = 3$. So, $3 = 1_S \neq 1_R$. 😄

Question: 32

Let R be a ring. Define the center of R to be

$$Z(R) = \{a \in R : ar = ra \text{ for all } r \in R\}.$$

Prove that $Z(R)$ is a commutative subring of R.

Solution: Let $a, b \in Z(R)$. We have that $abr = arb = rab \forall r \in R$. We also have that $(a-b)r = ar - br = ra - rb = r(a-b) \forall r \in R$. Therefore, $ab, (a-b) \in Z(R)$. So, $Z(R)$ is a subring of R. By definition, the center if a ring is commutative. Therefore, $Z(R)$ is a commutative subring of R. 😄

Question: 35

Let R be a ring with identity.

a. Let u be a unit in R. Define a map $i_u : R \to R$ by $r \mapsto uru^{-1}$. Prove that i_u is an automorphism of R. Such an automorphism of R is called an inner automorphism of R. Denote the set of all inner automorphisms of R by $\text{Inn}(R)$.

b. Denote the set of all automorphisms of R as $\text{Aut}(R)$. Prove that $\text{Inn}(R)$ is a normal subgroup of $\text{Aut}(R)$.

c. Let $U(R)$ be the group of units in R. Prove that the map

$$\phi : U(R) \to \text{Inn}(R)$$

defined by $u \mapsto i_u$ is a homomorphism. Determine the kernel of ϕ.

d. Compute $\text{Aut}(\mathbb{Z})$, $\text{Inn}(\mathbb{Z})$, and $U(\mathbb{Z})$.

Solution:

a. $\forall a, b \in R$, we have that

$$\begin{aligned} i_u(a)i_u(b) &= (uau^{-1})(ubu^{-1}) \\ &= ua(u^{-1}u)bu^{-1} \\ &= uabu^{-1} \\ &= i_u(ab) \end{aligned}$$

Also,

$$\begin{aligned} i_u(a) + i_u(b) &= (uau^{-1}) + (ubu^{-1}) \\ &= u(a+b)u^{-1} \\ &= i_u(a+b) \end{aligned}$$

Now, for injectivity,

$$\begin{aligned} i_u(a) &= i_u(b) \\ uau^{-1} &= ubu^{-1} \\ a &= b \text{ by cancellation laws.} \end{aligned}$$

For surjectivity,

$$\begin{aligned} \forall a \in R, i_u(u^{-1}au) &= uu^{-1}auu^{-1} \\ &= (uu^{-1})a(uu^{-1}) \\ &= a \end{aligned}$$

So, i_u is a bijective homomorphism and is therefore an automorphism of R. 😄

b. We know that $e = i_e \in \text{Inn}(R)$. For closure and inverse, let $i_u, i_v \in \text{Inn}(R)$ and $r \in R$. Starting with inverse, we can see that

$$\begin{aligned} i_u^{-1}(r) &= u^{-1}ru \\ &= i_{u^{-1}}(r) \end{aligned}$$

Then for closure, we have that

$$\begin{aligned} i_u \circ i_v(r) &= i_u(vrv^{-1}) \\ &= uvrv^{-1}u^{-1} \\ &= uvr(uv)^{-1} \\ &= i_{uv}(r) \in \text{Inn}(R) \end{aligned}$$

To show that $\text{Inn}(R)$ is normal in $\text{Aut}(R)$, we have to show that $i_u \circ i_v \circ i_u^{-1}(x) \in \text{Inn}(R)$ for all $u, v \in U(R)$ and $x \in R$.

$$\begin{aligned} i_u \circ i_v \circ i_u^{-1}(x) &= i_u \circ i_v(u^{-1}xu) \\ &= i_u(vu^{-1}xuv^{-1}) \\ &= uvu^{-1}xuv^{-1}u^{-1} \\ &= i_{uvu^{-1}}(x) \in \text{Inn}(R) \end{aligned}$$ 😄

c. Let $u, v \in U(R)$. We have that

$$\begin{aligned}
\phi(u) \circ \phi(v)(r) &= i_u \circ i_v(r) \\
&= i_u(vrv^{-1}) \\
&= uvrv^{-1}u^{-1} \\
&= i_{uv}(r) \\
&= \phi(uv)(r) \quad 😄
\end{aligned}$$

$$\begin{aligned}
\ker(\phi) &= \{u \in U(R) : \phi(u) = i_u = e\} \\
&= \{u \in U(R) : uru^{-1} = r \forall r \in R\} \\
&= \{u \in U(R) : ur = ru \forall r \in R\} \\
&= U(R) \cap Z(R)
\end{aligned}$$

d. $\mathbb{Z}$ is generated by 1 and -1. Therefore, $\text{Aut}(\mathbb{Z}) = \{x \mapsto x, x \mapsto -x\}$.

Analyzing both automorphisms, we see that their inner automorphisms are the same. As such, $\text{Inn}(\mathbb{Z}) = \{x \mapsto x\}$. Trivially, $U(\mathbb{Z}) = \{1, -1\}$.

Question: 36

Let R and S be arbitrary rings. Show that their Cartesian product is a ring if we define addition and multiplication in $R \times S$ by

a. $(r, s) + (r', s') = (r + r', s + s')$

b. $(r, s)(r', s') = (rr', ss')$

Solution: Let $T = R \times S$ and let $(a, b), (c, d), (e, f) \in T$. To start, we know that $a + c \in R$ and $b + d \in S$. So we can demonstrate cloure.

$$(a, b) + (c, d) = (a + c, b + d) \in T,$$

Now we should show associativity with addition:

$$\begin{aligned}
(a, b) + [(c, d) + (e, f)] &= (a, b) + (c + e, d + f) \\
&= (a + c + e, b + d + f) \\
&= (a + c, b + d) + (e, f) \\
&= [(a, b) + (c, d)] + (e, f)
\end{aligned}$$

If $0_R \in R$ and $0_S \in S$ and they are the identities, then we have the following:

$$\begin{aligned}
(a, b) + (0_R, 0_S) &= (a + 0_R, b + 0_S) \\
&= (a, b) \\
(0_R, 0_S) + (a, b) &= (0_R + a, 0_S + b) \\
&= (a, b)
\end{aligned}$$

Now, we will show that addition is commutative.

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

Next, we will show that multiplication is closed.

$$(a,b)(c,d) = (ac,bd) \in T$$

Next, we will show that multiplication is associative.

$$\begin{aligned}(a,b)[(c,d)(e,f)] &= (a,b)(ce,df)\\ &= (a[ce],b[df])\\ &= ([ac]e,[bd]f)\\ &= [(a,b)(c,d)](e,f)\end{aligned}$$

Now we just need to prove left and right distributivity of multiplication over addition.

$$\begin{aligned}(a,b)[(c,d)+(e,f)] &= (a,b)(c+e,d+f)\\ &= (a[c+e],b[d+f])\\ &= ([ac]+[ae],[bd]+[bf])\\ &= (a,b)(e,f)+(c,d)(e,f)\end{aligned}$$

$$\begin{aligned}[(a,b)+(c,d)](e,f) &= (a+c,b+d)(e,f)\\ &= ([a+c]e,[b+d]f)\\ &= ([ae]+[ce],[bf]+[df])\\ &= (a,b)(e,f)+(c,d)(e,f)\end{aligned}$$