Tutorial #5: Rings and Fields

Exercise 0:

a) Since $a0 = a(0+0) = a0 + a0$. Thus, $a0 = 0$.
Since $0a = (0+0)a = 0a + 0a$. Thus, $0a = 0$.
Therefore, $a0 = 0a = 0$.

b) We have:

$$ab + (-a)b = (a + (-a))b = 0b = 0.$$
$$ab + a(-b) = a(b + (-b)) = a0 = 0.$$
$$ab - ab = ab + (-ab) = 0$$

The inverse of ab is unique as R is a abelian group under addition.
Thus, $(-a)b = a(-b) = -ab$.

c) We have:

$$(-a)(-b) + (-a)b = (-a)(-b+b) = 0.$$
$$ab + (-a)b = ab - ab = 0.$$

The inverse of $(-a)b$ is unique as R is an abelian group under addition operation. Hence, $(-a)(-b) = ab$.

Exercise 1:

- $7\mathbb{Z}$

  i) Let $a, b, c \in 7\mathbb{Z}$, $\exists i, j$ and $k \in \mathbb{Z}$ such that $a = 7i, b = 7j, c = 7k$.

  $$(a+b)+c = (7i+7j)+7k = 7(i+j)+7k = 7(i+j+k).$$
  $$a+(b+c) = 7i+(7j+7k) = 7i+7(j+k) = 7(i+j+k).$$

Hence, $(a+b)+c = a+(b+c)$, the ring is associative under addition operation.

ii) There exist $e = 0$ such that $a+e = 7i+0 = 7i = a$. Thus, ring R has identity element under addition operation.

iii) There exist $a^{-1} = -7i$ such that $a+a^{-1} = 7i-7i = 0 = e$. ring R has inverse element under addition operation.

iv) Since $a+b = 7(i+j) = 7(j+i) = b+a$, ring R is commutative under addition operation.

v) Since $ab = 7i \times 7j = 7j \times 7i = ba$, ring R is commutative under multiplication operation.

vi) Since $(a+b)c = (7i+7j)7k = 49ik + 49jk = ac+bc$, ring R is multiplicative distributive associated with addition operation.

Conclusion: Hence, $7\mathbb{Z}$ is a ring.

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

i) Let $a, b, c \in \mathbb{Q}(\sqrt{2})$, $\exists i, j, k, l, m, n$ such that: $\begin{cases} a = i + \sqrt{2}l \\ b = j + \sqrt{2}m \\ c = k + \sqrt{2}n \end{cases}$

$(a+b)+c = (i+j+\sqrt{2}(l+m))+k+\sqrt{2}n = i+j+k+\sqrt{2}(l+m+n)$
$a+(b+c) = i+\sqrt{2}l+(j+k+\sqrt{2}(m+n)) = i+j+k+\sqrt{2}(l+m+n)$
Hence, ring R is associative under addition operation.

ii) There exists $e = 0$ such that $a+e = (i+\sqrt{2}l)+0 = i+\sqrt{2}l = a$. Thus, ring R has identity element under addition operation.

iii) There exists such $a^{-1} = -i - \sqrt{2}l$ satisfies $a + a^{-1} = e$. Thus ring R has inverse element under addition operation.

iv) Since $a+b = i+j+\sqrt{2}(l+m) = j+i+\sqrt{2}(m+l) = b+a$. Thus, ring R is commutative under addition operation.

v) Since $ab = (i+\sqrt{2}l)(j+\sqrt{2}m) = ij + \sqrt{2}(lj+im) + 2lm = ji + \sqrt{2}(mi+jl) + 2ml = (j+\sqrt{2}m)(i+\sqrt{2}l) = ba$, ring R is commutative under multiplication operation.

vi) Since $(a+b)c = (i+\sqrt{2}l + j\sqrt{2}m)(k+\sqrt{2}n) = ... = ab + ac$, ring R is multiplicative distributive associated with addition operation.

Exercise 2:

Prove that: R is a commutative ring. Given that R is a ring and $a^2 = a$ for every $a \in \mathbb{R}$.
Proof:
With $a = a^2 (\forall a \in R)$, we can prove that:

$$\begin{aligned} a + a &= (a+a)^2 \\ a + a &= a^2 + a^2 + a^2 + a^2 \\ a + a &= a + a + a + a \\ a + a &= 0 \\ a &= -a \end{aligned}$$

Let $a, b \in$ R, since R is a ring, R is also an abelian group under addition operation. Therefore, $(a+b) \in$ R,

$$\begin{aligned} (a+b)^2 &= a + b \\ a^2 + ab + ba + b^2 &= a^2 + b^2 \\ ab &= -ba \end{aligned}$$

Since $b = -b, \forall b \in$ R, we can conclude that $ab = ba$. Hence, ring R is commutative.

Exercise 3:

Prove that: $\phi(1)$ is identity element of R' if R is a ring with identity element 1 and ϕ is a homomorphism of R onto R'.
Proof: Since ϕ is homomorphism, we have: $\phi(ab) = \phi(a)\phi(b)$
Let $x \in R$ and 1_R be identity element of R, we have $1_R * x = x \; \forall x \in R$.

$$\phi(x) = \phi(1_R * x) = \phi(1_R)\phi(x)$$

Thus, $\phi(1_R)$ is the identity element of R'.

Exercise 4:

Prove that: Z(R) is a subring of R, Z(R) $= \{x \in \mathbb{R} | xy = yx, \forall y \in \mathbb{R}\}$

i) It's trivial that Z(R) $\neq \emptyset$

ii) Let $a, b \in$ Z(R), thus $at = ta, bt = tb,\ \forall t \in \mathbb{R}$.

$$\begin{aligned} atb &= atb \\ (at)b &= a(tb) \\ (ta)b &= a(bt) \\ t(ab) &= (ab)t. \end{aligned}$$

Thus, $ab \in Z(R)$.

iii) Since $a, b \in$ Z(R),

$$\begin{aligned} at - bt &= at - bt \\ at + (-b)t &= ta + t(-b) \\ (a + (-b))t &= t(a + (-b)) \\ (a - b)t &= t(a - b) \end{aligned}$$

Thus, $(a - b) \in Z(R)$.

Conclusion: By the definition of subring, Z(R) is a subring of $\mathbb{R}$.

Exercise 5:

General formula: $1 + (-1)^{n-1}x^n = (1 + x)\sum_{i=0}^{n-1}(-x)^i$
It's trivial that with $n \equiv 1 \pmod 2$,

$$1 = x^n + 1 = x^n(-1)^{n-1} + 1 = (x + 1)\sum_{i=0}^{n-1}(-x)^i$$

Since $x \in \mathbb{R}$ and $i \in \mathbb{N}$, there exists $\sum_{i=0}^{n-1}(-x)^i \in \mathbb{R}$. Thus, $(x+1)$ is an unit.

Exercise 6:

Prove that: If a ring is isomorphic to a field, then that ring is a field.
Proof: Let $f : R \to F$ be an isomorphism from ring R to field F.

i) Let $a, b \in$ R, since R is a ring, $ab \in$ R. Since F is a field, F is multiplicative commutative ($f(a)f(b) = f(b)f(a)$). Thus, by the definition of homomorphism, we have:

$$f(ab) = f(a)f(b) = f(b)f(a) = f(ba)$$

Since f is injective, we can conclude that $ab = ba$ and ring R is commutative under multiplication.

ii) Let 1_F be multiplicative identity of F, $\forall a \in$ R,and f is isomorphism:

$$f^{-1}(1_F)*a = f^{-1}(1_F)*f^{-1}(f(a)) = f^{-1}(1_F*f(a)) = f^{-1}(f(a)) = a$$

Thus, $1_R = f^{-1}(1_F)$ is multiplicative identity of R.

iii) Since F is a field, $\forall a \neq 0 \in$ R, we have:

$$\begin{aligned} f^{-1}(a) * f(a) &= e \\ \frac{1_F}{f(a)} f(a) &= 1_F \\ f^{-1}\left(\frac{1_F}{f(a)} f(a)\right) &= 1_R \\ f^{-1}\left(\frac{1_F}{f(a)}\right) f^{-1}(f(a)) &= 1_R \\ f^{-1}\left(\frac{1_F}{f(a)}\right) a &= 1_R \end{aligned}$$

Thus, $\frac{1_R}{a} = f^{-1}\left(\frac{1_F}{f(a)}\right)$ is multiplicative inverse of R.

Conclusion: With i), ii) and iii), we conclude that R is also a field.

Exercise 7:

Prove that: $(g \circ f) : A \to C$ is isomorphism if $f : A \to B$ and $g : B \to C$ are isomorphisms.

f and g are isomorphisms $\rightarrowtail \begin{cases} f(a)f(b) & = f(ab) \\ g(a)g(b) & = g(ab) \end{cases}$ Thus, we have:

$$(f \circ g)(a) * (f \circ g)(b) = f(g(a)) * f(g(b)) = f(g(a) * g(b)) = f(g(ab)) = (f \circ g)(ab)$$

In addition, since both f and g is bijective, $f \circ g$ is also bijective. **Conclusion:** $f \circ g$ is isomorphism.