Rings and Fields

Def. A **ring** $(R, +, \cdot)$ is a set R with two binary operations $+$ and $\cdot$, called addition and multiplication, defined on R such that the following axioms are satisfied.

1) $(R, +)$ is an abelian group
2) Multiplication is associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (and R is closed under multiplication).
3) For all $a, b, c \in R$, the left and right distributive laws hold:
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$(b + c) \cdot a = (b \cdot a) + (c \cdot a)$$

Ex. Any subset of $\mathbb{C}$ that is a group under $+$ is a ring under the usual addition and multiplication. Thus $(\mathbb{C}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, and $(\mathbb{Z}, +, \cdot)$ are rings. We will refer to these rings as $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{Z}$ where the usual addition and multiplication are understood.

Ex. Let R be any ring and let $M_n(R)$ be the set of all $n \times n$ matrices having elements of R as entries. $M_n(R)$ is a ring with the usual addition and multiplication of matrices. We can see this because:

1) $M_n(R)$ is an abelian group under addition
2) Matrix multiplication is associative (and $M_n(R)$ is closed under multiplication)
3) Matrix addition and multiplication are distributive:
$$A \cdot (B + C) = (A \cdot B) + (A \cdot C)$$
$$(B + C) \cdot A = (B \cdot A) + (C \cdot A).$$

In particular $M_n(\mathbb{C})$, $M_n(\mathbb{R})$, $M_n(\mathbb{Q})$, and $M_n(\mathbb{Z})$ are rings.

Notice in this example $+$ is commutative (which is required by the definition of a ring) but matrix multiplication is not commutative for $n \geq 2$. A ring where $\cdot$ is commutative is called a **commutative ring**.

Ex. Show F, the set of all functions $f: \mathbb{R} \to \mathbb{R}$, is a ring with the usual addition and multiplication of functions.

Define multiplication on F by: $(f \cdot g)(x) = f(x)g(x)$.

With the definitions of $+$ and $\cdot$, F is a ring since:

1) We know $(F, +)$ is an abelian group under the usual addition of functions: $(f + g)(x) = f(x) + g(x)$.

2) $\big((f \cdot g) \cdot h\big)(x) = (f \cdot g)(x) \cdot h(x) = f(x) \cdot g(x) \cdot h(x)$

$$\big(f \cdot (g \cdot h)\big) = f(x) \cdot (g \cdot h)(x) = f(x) \cdot g(x) \cdot h(x)$$

and F is closed under multiplication.

3) $f \cdot (g + h)(x) = f(x)\big(g(x) + h(x)\big) = f(x)g(x) + f(x)h(x)$

$$= f \cdot g + f \cdot h$$

$$(g + h) \cdot f(x) = \big(g(x) + h(x)\big) \cdot f(x) = g(x)f(x) + h(x)f(x)$$

$$= g \cdot f + h \cdot f.$$

Notice that if we defined multiplication as composition of functions:
i.e. $f \cdot g = (f \circ g)(x)$, F would not be a ring since this multiplication is not distributive. For example, let $f(x) = x^2, \quad g(x) = x, \quad h(x) = x$.

$$f \circ (g + h) = f \circ (2x) = (2x)^2 = 4x^2$$

$$f \circ g + f \circ h = x^2 + x^2 = 2x^2$$

So $\quad f \circ (g + h) \neq f \circ g + f \circ h$.

Ex. Show that $n\mathbb{Z} = \{x \in \mathbb{Z} |\ x = ny \text{ for } y \in \mathbb{Z}\}$ is a ring.

$n\mathbb{Z} = \{x \in \mathbb{Z} |\ x = ny \text{ for } y \in \mathbb{Z}\}$ is an abelian group under the usual addition.

$n\mathbb{Z}$ is also closed under the usual multiplication since $x, y \in n\mathbb{Z}$ means $x = na,\ \ y = nb$ for all $a, b \in \mathbb{Z}$, so $xy = (na)(nb) = n(anb)$. Since $anb \in \mathbb{Z}$, $xy \in n\mathbb{Z}$.

The usual multiplication in $\mathbb{Z}$ is closed, associative and satisfies the left and right distributive laws. Thus, these also work in $n\mathbb{Z}$.

Thus, $n\mathbb{Z}$ is a ring.

Ex. $(\mathbb{Z}_n, +)$ is an abelian group. If we define $a \cdot b = (ab)\ (mod\ n)$, $\mathbb{Z}_n$ is a ring (we will show this later).

For example, in $\mathbb{Z}_{12}$,

$$7 \cdot 8 = \big(7(8)\big)\ (mod\ 12)$$
$$= 56\ \ (mod\ 12)$$
$$= 8.$$

Notice that this is a little "weird". In a group if $a \cdot b = b$ then a is the identity element. That's not the case, in general, for rings.

Ex. If $R_1, R_2, \ldots, R_n$ are rings, we can form $R_1 \times R_2 \times \ldots \times R_n$ of all ordered n-tuples $(r_1, r_2, \ldots, r_n)$, where $r_i \in R_i$. We define addition and multiplication of n-tuples by component (as we did with groups). Since each component satisfies the ring axioms, so does the direct product $R_1 \times R_2 \times \ldots \times R_n$. Thus $R_1 \times R_2 \times \ldots \times R_n$ is a ring and is called the **direct product of rings R_i.**

We will write $n \cdot a = a + a + \cdots + a$, n-times. Note this is not necessarily the multiplication in the R. For example, if $R = M_2(\mathbb{R})$ and $A \in R$, then $3A = A + A + A$. In fact, $3A$ wouldn't even make sense for matrix multiplication (at least as written) because 3 is not a 2×2 matrix.

If $n < 0$, an integer, $n \cdot a = (-a) + (-a) + (-a) + \cdots + (-a)$.

We define $0 \cdot a = 0$, where the 0 on the left hand side is $0 \in \mathbb{Z}$, and 0 on the right hand side is the $0 \in R$ (which might not be a number. For example, It could be a matrix or a function).

Theorem: If R is a ring with additive identity 0, then for any $a, b \in R$:

1) $0a = a0 = 0$.
2) $a(-b) = (-a)b = -(ab)$.
3) $(-a)(-b) = ab$.

Def. For rings R and R', a map $\phi: R \to R'$ is a **ring homomorphism** if for all $a, b \in R$.

1) $\phi(a + b) = \phi(a) + \phi(b)$
2) $\phi(ab) = \phi(a)\phi(b)$.

Note: Since ϕ is also a group homomorphism of $(R, +)$ to $(R', +')$ all of the properties of group homomorphism hold. In particular, ϕ is 1-1 if, and only if, $\ker \phi = \{a \in R \mid \phi(a) = 0'\}$ is $\{0\} \in R$.

Ex. Let F be the ring of all functions $f: \mathbb{R} \to \mathbb{R}$. For every $a \in \mathbb{R}$ we have the evaluation homomorphism $\phi_a: F \to \mathbb{R}$ by $\phi_a(f) = f(a)$.

$$\phi_a(f+g) = (f+g)(a) = f(a) + g(a) = \phi_a(f) + \phi_a(g).$$

$$\phi_a(fg) = (fg)(a) = f(a)g(a) = \phi_a(f)\phi_a(g).$$

This homomorphism is important because finding a root of an equation is the same as finding $p \in \mathbb{R}$ (or $\mathbb{C}$) such that

$$\phi_p(f) = f(p) = 0.$$

So f is in the kernel of ϕ_p.

Ex. Show that $\phi: \mathbb{Z} \to \mathbb{Z}_n$ where $\phi(z) = z \ (mod\ n)$ is a ring homomorphism for each positive integer n.

From group theory we know:

$$\phi(z+w) = \phi(z) + \phi(w).$$

To show $\phi(zw) = \phi(z)\phi(w)$ write:

$z = q_1 n + r_1$ and $w = q_2 n + r_2$ where $0 \le r_1, r_2 < n$.

$$zw = (q_1 n + r_1)(q_2 n + r_2) = n(q_1 q_2 n + r_1 q_2 + r_2 q_1) + r_1 r_2.$$

Thus, $\phi(zw) = r_1 r_2 \ (mod\ n)$.

But since $0 \le r_1, r_2 < n$:

$r_1 = \phi(z)$ and $r_2 = \phi(w) \implies \phi(zw) = \phi(z)\phi(w)$.

Note: From group theory we know the factor group $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$. The same will turn out to be true for $\mathbb{Z}/n\mathbb{Z}$ as a factor ring.

Def: An **isomorphism** $\phi: R \to R'$ from a ring R to a ring R' is a ring homomorphism that is 1-1 and onto.

Not every group isomorphism (or homomorphism) is a ring isomorphism (or homomorphism).

Ex. Prove that the rings $\mathbb{Z}$ and $5\mathbb{Z}$ are not isomorphic (although they are isomorphic as groups under addition by $\phi: \mathbb{Z} \to 5\mathbb{Z},\ \phi(x) = 5x$).

Assume $\phi: \mathbb{Z} \to 5\mathbb{Z}$ is a ring isomorphism.

Then, $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$.

Then $\quad \phi(2a) = \phi(a) + \phi(a) = 2\phi(a)$.

But $\quad \phi(2a) = \phi(2)\phi(a)$

$$\Rightarrow \phi(2) = 2$$

But $2 \notin 5\mathbb{Z}$, thus ϕ cannot be an isomorphism.

For example, if $a = 3$ and $\phi(x) = 5x$:

$$\phi(6) = \phi(3 + 3) = \phi(3) + \phi(3) = 15 + 15 = 30$$

$$\phi(6) = \phi(2 \cdot 3) = \phi(2) \cdot' \phi(3) = 10 \cdot' 15 = 150.$$

which is a contradiction, so ϕ is not a ring isomorphism.

Fields

Many rings have a multiplicative identity element. For example, 1 is the multiplicative identity element (i.e. $1 \cdot x = x$ for all $x \in R$) for the rings $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{Z}$. But $2\mathbb{Z}$ is a ring and it doesn't have a multiplicative identity element.

Def. A ring with a multiplicative identity element is a **ring with unity**. We will call this multiplicative identity element 1 (although it could be a matrix or function).

Ex. If $GCD(q, r) = 1$ for positive integers q and r, show that the rings $\mathbb{Z}_{qr}$ and $\mathbb{Z}_q \times \mathbb{Z}_r$ are isomorphic.

Additively, $\mathbb{Z}_{qr}$ and $\mathbb{Z}_q \times \mathbb{Z}_r$ are both cyclic abelian groups of order qr. 1 is a generator for $\mathbb{Z}_{qr}$ and $(1,1)$ is a generator for $\mathbb{Z}_q \times \mathbb{Z}_r$.

If we let $\phi: \mathbb{Z}_{qr} \to \mathbb{Z}_q \times \mathbb{Z}_r$ by $\phi(n \cdot 1) = n \cdot (1,1)$ this is an additive group isomorphism since ϕ clearly 1-1, onto, and

$$\begin{aligned}\phi(n+m) &= (n+m)(1,1)\\ &= n(1,1) + m(1,1)\\ &= \phi(n) + \phi(m).\end{aligned}$$

1 is the multiplicative unity in $\mathbb{Z}_{qr}$ and $(1,1)$ is the multiplicative unity in $\mathbb{Z}_q \times \mathbb{Z}_r$. So:

$$\phi(nm) = nm(1,1) = [n(1,1)] \cdot [m(1,1)] = \phi(n)\phi(m).$$

Note: a direct product $R_1 \times R_2 \times \ldots \times R_n$ of rings is commutative or has unity if, and only if, each R_i is commutative or has unity.

Def. Let R be a ring with unity $1 \neq 0$. An element u in R is a **unit** of R if it has a multiplicative inverse in R. If every non-zero element of R is a unit, then R is a **division ring** (or **skew field**). A **field** is a commutative division ring. A non-commutative division ring is called a "**strictly skew field**."

Ex. Find the units of $\mathbb{Z}_6$.

$a \in \mathbb{Z}_6$ is a unit of $\mathbb{Z}_6$ if there exists a $b \in \mathbb{Z}_6$ such that

$ab = (ab)\ (mod\ 6) = 1.$

1 is a unit since $1 \cdot 1 = 1$.

No even number can be a unit in $\mathbb{Z}_6$ because if a is even, then $ab \in \mathbb{Z}$ is even (if b is an integer) so $ab\ (mod\ 6) \neq 1$. Thus, 2 and 4 are not units.

$(3)(2)\ (mod\ 6) = 0, \quad (3)(3)\ (mod\ 6) = 3,$

$(3)(4)\ (mod\ 6) = 0, \quad (3)(5)\ (mod\ 6) = 3.$

So 3 is not a unit.

$(5)(5)\ (mod\ 6) = 1$ so 5 is its own inverse and 5 is a unit.

Thus, 1 and 5 are the only units in $\mathbb{Z}_6$. Thus, $\mathbb{Z}_6$ is not a field. We will see later that the only units in $\mathbb{Z}_n$ are $m \in \mathbb{Z}_n$ such that $GCD(m, n) = 1$.

Ex. Show that $\mathbb{Z}_3$ is a field.

$\mathbb{Z}_3$ is a commutative ring and $1, 2 \ \ (2 \cdot 2 = 1 \ (mod\ 3))$ are units.

In fact, $\mathbb{Z}_p$, where p is a prime number, is a field because $GCD(m, p) = 1$ where p is prime and m is an integer $1 \leq m < p$, so all elements except 0 are units.

Ex. $\mathbb{Z}$ is not a field because 3, in particular, has no multiplicative inverse (neither do any other elements of $\mathbb{Z}$ except 1 and -1).

Analogous to subgroups, a **subring** R' of a ring R is a subset of R and is a ring under $+$ and $\cdot$ defined on R. A **subfield** K' of a field K is a subset of K and is a field under $+$ and $\cdot$ defined on K.