Class 19

April 1, 2024

Rings

Now we are going to talk about rings. The algebra of rings will probably be more familiar than the algebra of groups, as you have worked with rings many times throughout previous math classes. The name ring comes from David Hilbert. He meant the word ring as in a spy ring, rather than as the geometric object.

Def

A Ring R is a set with two binary operations, addition $(a+b)$ and multiplication (ab or $a*b$), that obey the following axioms $\forall a, b, c \in R$:

1. $a+b=b+a$ (Commutativity of Addition)
2. $(a+b)+c=a+(b+c)$ (Associativity of Addition)
3. $\exists 0 \in R$ such that $a+0=a\ \forall a \in R$ (Identity under Addition)
4. $\exists -a \in R$ such that $a+(-a)=0$ (Inverses under Addition)
5. $a\,(bc)=(ab)\,c$ (Associativity of Multiplication)
6. $a\,(b+c)=ab+ac$ and $(b+c)\,a=ba+ca$ (Distributive Laws)

Note that the addition and multiplication rules need not be the standard addition and multiplication rules. These binary operations will be defined for the specific ring. Equivalently, R is an abelian group under addition and obeys 5 and 6.

Examples

Here are some examples of rings.

1) $R_1=\mathbb{Z}$ under the usual rules of addition and multiplication (We know $\mathbb{Z}$ is an abelian group under addition already. The real numbers are associative and distributive, so the integers must be too).

2) $R_2=M_{2\times 2}(\mathbb{R})$ the set of 2×2 matrices under the usual rules of matrix addition and multiplication.

3) $R_3=\mathbb{Z}[x]$ the set of all polynomials with variable x and integer coefficients under the usual rules of addition and multiplication

4) $R_4=3\mathbb{Z}$ the set of all integers divisible by 3.

Pf

We will prove that **3)** and **4)** are rings.

3)

Let $a, b, c \in R_3$. For convenience, suppose $a=\sum_{k=0}^{\infty} a_k x^k$, $b=\sum_{k=0}^{\infty} b_k x^k$, $c=\sum_{k=0}^{\infty} c_k x^k$ where $a_k, b_k, c_k \in \mathbb{Z}$. Let's show each axiom! First, let's show $+$ and $*$ are binary operations.

Binary Operations $a+b=\sum_{k=0}^{\infty} a_k x^k+\sum_{k=0}^{\infty} b_k x^k=\sum_{k=0}^{\infty}(a_k+b_k)\,x^k \in R_3$ as $a_k+b_k \in \mathbb{Z}$

$ab=\left(\sum_{k=0}^{\infty} a_k x^k\right)\left(\sum_{k=0}^{\infty} b_k x^k\right)=\sum_{k=0}^{\infty}\sum_{i=0}^{k}(a_l b_{k-l})\,x^k \in R_3$ as $\sum_{i=0}^{k}(a_l b_{k-l}) \in \mathbb{Z}$

1) $a+b=\sum_{k=0}^{\infty} a_k x^k+\sum_{k=0}^{\infty} b_k x^k=\sum_{k=0}^{\infty} b_k x^k+\sum_{k=0}^{\infty} a_k x^k=b+a$

2) $(a+b)+c=\left(\sum_{k=0}^{\infty} a_k x^k+\sum_{k=0}^{\infty} b_k x^k\right)+\sum_{k=0}^{\infty} c_k x^k=\sum_{k=0}^{\infty} a_k x^k+\left(\sum_{k=0}^{\infty} b_k x^k+\sum_{k=0}^{\infty} c_k x^k\right)=a+(b+c)$

3) $a+0=\sum_{k=0}^{\infty} a_k x^k+0=\sum_{k=0}^{\infty} a_k x^k=a$ (here, 0 is the polynomial where each coefficient is $0 \in \mathbb{Z}$)

4) $-a=-\sum_{k=0}^{\infty} a_k x^k=\sum_{k=0}^{\infty} -a_k x^k$. As each $-a_k \in \mathbb{Z}$, then $-a \in R_3$

5) $(ab)\,c = \left(\left(\sum_{k=0}^{\infty} a_k x^k\right)\left(\sum_{k=0}^{\infty} b_k x^k\right)\right)\left(\sum_{k=0}^{\infty} c_k x^k\right) = \left(\sum_{k=0}^{\infty} a_k x^k\right)\left(\left(\sum_{k=0}^{\infty} b_k x^k\right)\left(\sum_{k=0}^{\infty} c_k x^k\right)\right) = a\,(bc)$

6) $a\,(b+c) = \left(\sum_{k=0}^{\infty} a_k x^k\right)\left(\left(\sum_{k=0}^{\infty} b_k x^k\right) + \left(\sum_{k=0}^{\infty} c_k x^k\right)\right) = \left(\sum_{k=0}^{\infty} a_k x^k\right)\left(\sum_{k=0}^{\infty} b_k x^k\right) + \left(\sum_{k=0}^{\infty} a_k x^k\right)\left(\sum_{k=0}^{\infty} c_k x^k\right) = ab + ac$

$(b+c)\,a = \left(\left(\sum_{k=0}^{\infty} b_k x^k\right) + \left(\sum_{k=0}^{\infty} c_k x^k\right)\right)\left(\sum_{k=0}^{\infty} a_k x^k\right) = \left(\sum_{k=0}^{\infty} b_k x^k\right)\left(\sum_{k=0}^{\infty} a_k x^k\right) + \left(\sum_{k=0}^{\infty} c_k x^k\right)\left(\sum_{k=0}^{\infty} a_k x^k\right) = ba + ca$

4)

Let $a, b, c \in R_4$. For convenience, suppose $a = 3n$, $b = 3m$, $c = 3k$ where $n, m, k \in \mathbb{Z}$. Let's show each axiom! First, let's show $+$ and $*$ are binary operations.

Binary Operations $a + b = 3n + 3m = 3\,(n+m) \in R_4$ as $n + m \in \mathbb{Z}$

$ab = (3n)\,(3m) = 9nm = 3\,(3mn) \in R_4$ as $(3mn) \in \mathbb{Z}$

1) $a + b = 3n + 3m = 3m + 3n = b + a$

2) $(a+b) + c = (3n + 3m) + 3k = 3n + (3m + 3k)$

3) $a + 0 = 3n + 0 = 3n = a$ (here, $0 = 3 * 0$ so $0 \in R_4$)

4) $-a = -3n = 3\,(-n)$. As $-3 \in \mathbb{Z}$, then $-a \in R_4$

5) $(ab)\,c = (3n * 3m)\,3k = 3n\,(3m * 3k)$

6) $a\,(b+c) = 3n\,(3m + 3k) = 3n * 3m + 3n * 3k = ab + ac$

$(b+c)\,a = (3m + 3k)\,3n = 3m * 3n + 3k * 3n = ba + ca$

Properties of Rings

Notice that rings are not required to have a multiplicative identity. If a ring has a multiplicative identity, we usually denote this element as 1. The multiplicative identity is also called a unity and a ring with a multiplicative identity is also called a ring with unity. Any element that has a multiplicative inverse is called a unit (note R needs a unity for R to have units). Not every ring is commutative under multiplication. Rings that are commutative under multiplication are called commutative rings. Let's see which of our example rings have which properties:

Examples

1) R_1 is a commutative ring with unity. The unity is 1 and the units are $1, -1$ as $1 * 1 = 1, (-1) * (-1) = 1$

2) R_2 is non-commutative ring with unity. The unity is the identity matrix I and the units are all invertible matrices.

3) R_3 is a commutative ring with unity. The unity is 1 and the units are $1, -1$

4) R_4 is a commutative ring without unity. The is not a unity as for any $a = 3n, b = 3m$ $ab = 9nm = 3\,(3nm) \neq 3n$ for all $n \neq 0$ for any m.

More Properties of Rings

If R is a ring, then for all $a, b, c \in R$

1. $a * 0 = 0 * a = 0$
2. $a\,(-b) = (-a)\,b = -\,(ab)$
3. $(-a)\,(-b) = ab$
4. $a\,(b-c) = ab - ac$ and $(b-c)\,a = ba - ca$

If R has unity 1, we also have

1. $(-1)\,a = -a$
2. $(-1)\,(-1) = 1$
3. 1 is unique

Pf

1)

$$a * 0 = a * (0 + 0) = a * 0 + a * 0$$

$$a * 0 - a * 0 = a * 0 + a * 0 - a * 0$$

$$0 = a * 0$$

Similarly

$$0 * a = (0 + 0) * a = 0 * a + 0 * a$$

$$0 * a - 0 * a = 0 * a + 0 * a - 0 * a$$

$$0 = 0 * a$$

2)

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

Thus $a(-b) = -ab$. Similarly

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

Thus $(-a)b = a(-b) = -ab$ as inverses are unique in a group.

3)

Using **2)**

$$(-a)(-b) = -((-a)b) = --(ab)$$

Recall for any group

$$--a = a$$

thus

$$(-a)(-b) = --(ab) = ab$$

4)

$$a(b - c) = ab + a(-c) = ab + -ac = ab - ac$$

$$(b - c)a = ba + (-c)a = ba + -ca = ba - ca$$

Now for the unity properties:

1)

$$(-1)a = -(1a) = -(a) = -a$$

2)

$$(-1)(-1) = -(-1 * 1) = -(-1) = --(1) = 1$$

3)

Let $1, 1'$ be unities. Then

$$1 = 1 * 1' = 1'$$

Thus $1 = 1'$ for all unities and 1 is unique.

Subrings

A ring contained entirely within another ring (under the same binary operations) is called a subring. This is analogous to how a subgroup is contained entirely within another group (assuming both share the same binary operation). There is a subring test: $S \subseteq R$ is a subring of R if S is closed under subtraction and multiplication. Symbolically, if $a, b \in S$

1. $a - b \in S$
2. $ab \in S$

There is not a common symbol for subrings, but in class, it was proposed that we use the symbol $S < \underline{\circledcirc} R$ if S is a subring of R.

Pf

If $a - b \in S$ this implies that S is a subgroup of R under addition, as this is the same as subgroup test 1. Ring axioms 5 and 6 are inherited from R as each element of S is an element of R and all elements of R obey ring axioms 5 and 6. The closure under multiplication of S implies that multiplication is a valid binary operation on S, thus our subring test is valid.

Examples

1. S_1 From the earlier rings, R_4 is a subring of R_1.
2. S_2 The set of all diagonal matrices is a subring of R_2 (but the set of all invertible matrices is not)
3. S_3 The set of all polynomials $\mathbb{Z}\left[x^2\right] \subseteq Z\left[x\right]$ is a subring of R_3

Pf

We will show 2. and 3. are indeed subrings.

2)

Using the subring test, let A, B be diagonal matrices. Then $A - B$ is diagonal (proof from linear algebra class). We also know AB is diagonal (proof from a linear algebra class). As S_2 is closed under subtraction and multiplication, it is a subring of R_2. Consider the invertible matrix $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $A - A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ but $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is not invertible, so S is not closed under subtraction.

3)

Let $a = \sum_{k=0}^{\infty} a_{2k} x^{2k}, b = \sum_{k=0}^{\infty} b_{2k} x^{2k}$. Then $a - b = \sum_{k=0}^{\infty} a_{2k} x^{2k} - \sum_{k=0}^{\infty} b_{2k} x^{2k} = \sum_{k=0}^{\infty} \left(a_{2k} - b_{2k}\right) x^{2k}$. As $a_{2k} - b_{2k} \in \mathbb{Z}$,then $a - b \in S_3$. For multiplication $ab = \sum_{k=0}^{\infty} \sum_{i=0}^{k} \left(a_{2l} b_{2k-2l}\right) x^{2k} \in S_3$ as $\sum_{i=0}^{k} \left(a_{2l} b_{2k-2l}\right) \in \mathbb{Z}$.