2 Rings

2.1 Rings: introduction and definition

Many of the sets we've come across in our study of groups are naturally endowed with two operations: the integers, the reals and the complex numbers, but also sets of matrices or functions. If the two operations (typically addition and multiplication) satisfy certain properties and "interact well" with each other then we say that the relevant set with the two operations forms a ring

Definition (Ring) A ring is a set R together with two operations called addition and multiplication ($+$ and $\cdot$) such that

(1) $(R,+)$ is an abelian group ← Remember, this means: $+$ is associative & commutative, $\exists\, 0 \in R$ (additive neutral element), $a \in R \Rightarrow -a \in R$.

(2) multiplication is associative

(3) for all $a,b,c \in R$ $\quad a(b+c) = ab+ac$, and $(a+b)c = ac+bc$ hold. } Distributive laws

(U) There exist $e \in R$ such that $e \cdot a = a \cdot e = a \quad \forall a \in R$

For us all rings will satisfy (U). This is often not included in the definition. A ring satisfying (U) is also called ring with unity or identity

Examples

1. The ring of integers $\mathbb{Z}$, with the usual addition and multiplication
2. The ring of rational numbers $\mathbb{Q}$, " "
3. The set of $n \times n$ matrices with real entries $M_n(\mathbb{R})$ forms a ring under addition and (matrix) multiplication
4. The set of all functions $f: \mathbb{R} \to \mathbb{R}$. Given f, g in this set
   $f+g$ and $f \cdot g$ are again functions $: \mathbb{R} \to \mathbb{R}$.
   Also, the function $0(x) = 0 \ \forall x$ is the zero of this ring
   and $1(x) = 1 \ \forall x$ is the (multiplicative) unity of this ring.
5. $\mathbb{Q}[x]$ = set of polynomials in x over $\mathbb{Q}$. An element of this set is a polynomial, an expression of the form
   $$a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$
   where d is a non-negative integer and $a_0, \ldots a_d \in \mathbb{Q}$.

Definition A ring is said to be commutative if $ab = ba$ for all $a,b \in R$

Note: the requirement is on the multiplication. $(R,+)$ is always an abelian group

Example 3. above is an example of non-commutative ring.
All the familiar sets of numbers form commutative rings.

The two operations have different properties - essentially because there is no requirement for $(R,\cdot)$ to form a group.

Properties (addition)

- $0 \in R$ is unique
- each element of R has a unique inverse
- if $a+b=a+c$ then $b=c$, and
- if $a+b=c+b$ then $a=c$

} already seen for gps

- each of the equations $a+x=b$ and $x+a=b$ admits a unique solution
- $-(-a)=a$; $-(a+b)=-a+(-b)$ ← we will simply write "$-b$" for "$+(-b)$"

In a general ring multiplication satisfies:

Properties (multiplication)

(1) $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$

(2) $a \cdot (-b) = (-a) \cdot b = -(ab)$ for all $a, b \in R$

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

(4) $(a-b)c = ac - bc$ & $a(b-c) = ab - ac$

It is easy to convince ourselves that all these properties hold. Let's try to convince ourselves that stronger properties (such as the cancellation laws) don't hold in general for multiplication in rings.

Examples (a) $R = (\{\text{real-valued functions of one real variable}\}, +, \cdot)$

Consider $f(x) = \begin{cases} x & \text{if } x \geq 0 \\ 0 & \text{if } x < 0 \end{cases}$ and $g(x) = \begin{cases} 0 & \text{if } x \geq 0 \\ x & \text{if } x < 0 \end{cases}$ (what is $f+g$?)

Then $(f \cdot g)(x) = \begin{cases} 0 & \text{if } x \geq 0 \\ 0 & \text{if } x < 0 \end{cases}$, that is $(f \cdot g)(x) = 0 \in R$

But $0 = 0 \cdot g$ (from multiplication properties (1) above)

so $(f \cdot g)(x) = (0 \cdot g)(x)$ but $f \neq 0$

(b) $R = (Mat_{2\times 2}(\mathbb{Z}), +, \cdot)$

Consider $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. $A^2 = A \cdot A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0 \in R$

So $A \cdot A = 0 \cdot A = A \cdot 0$ but $A \neq 0$

(c) $R = (\mathbb{Z}, +, \cdot)$ Here we know that whenever a, b, c are non-zero:

$ab = ac \Rightarrow b = c$

and (since R is commutative)

$ba = ca \Rightarrow b = c$

The difference between examples (a),(b) and (c) is the existence of elements such as f in (a) & A in (b) which multiplied with some other non-zero elements give the zero of the ring.

Definition

- An element $a \neq 0$ in a commutative ring R is called a zero divisor in R if there exist an element $b \neq 0$ in R such that $ab = 0$
- An element $A \neq 0$ in a non-commutative ring R is called a left (resp. right) zero divisor in R if there exist an element $B \neq 0$ in R such that

$AB = 0$ (left z.d.) (resp $BA = 0$ for a right z.d.)

Thus the ring of integers has no zero divisors. This fundamental property inspires the following definition.

Definition A commutative ring (with unity) and no zero divisors is called an integral domain

The rings of rational, real, complex numbers are integral domains.

The ring of functions $:\mathbb{R}\to\mathbb{R}$ is not an integral domain.

Theorem If D is an integral domain then the cancellation laws hold: if $a,b,c \in D$ with $a\neq 0$ then

$$ab = ac \Rightarrow b=c$$

and $ba = ca \Rightarrow b=c$.