Section 18 Rings and Fields

In early childhood you got used to having <u>two</u> algebraic operations, addition and multiplication. A <u>ring</u> is an algebraic object which emulates this.

<u>Definition</u> A ring is a set R with <u>two</u> binary operations, addition and multiplication, satisfying:

$\mathcal{R}_1$ $\langle R, + \rangle$ is an abelian group. with add. identity $0 \in R$.

$\mathcal{R}_2$ $(ab)c = a(bc)$

$\mathcal{R}_3$ distributive laws $\left\{ \begin{array}{l} a(b+c) = ab + ac \\ (a+b)c = ac + bc \end{array} \right.$

<u>Examples</u>: $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}$ $\mathbb{C}$ $3\mathbb{Z}$

<u>Ex</u> $M_n(\mathbb{R})$ = $m \times n$ matrices $(AB)C = A(BC)$, $A(B+C) = AB + AC$, etc.

<u>Ex</u> $F = \{ f : \mathbb{R} \to \mathbb{R} \}$ $(f+g)(x) = f(x) + g(x)$ $(fg)(x) = f(x)g(x)$.

<u>Ex</u> $\mathbb{Z}_n$

For instance, consider $\mathbb{Z}_3$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$$\begin{array}{ccc} 2(1+2) & = & 2\cdot 1 + 2\cdot 2 \\ \| & & \| \\ 2 \cdot 0 & = & 2 + 1 \end{array}$$

Actual proof that $\mathcal{R}_2$ and $\mathcal{R}_3$ hold for $\mathbb{Z}_n$ is going to wait until later. Just accept for now that $\mathbb{Z}_n$ <u>is</u> a ring.

<u>Theorem</u>: If R is a ring then:

1. $0a = 0 = a0 \quad \forall a \in \mathbb{R}$ $\qquad 0a = (0+0)a = 0a + 0a$
2. $a(-b) = (-a)(b) = -(ab)$ $\qquad (-a)(b) + ab = (-a + a)b = 0b = 0$
3. $(-a)(-b) = ab$

$\cancel{(-a)(-b) - ab} =$

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

Theorem If R_1 R_2 ... R_n are rings, then so is $\prod_{i=1}^{n} R_i = R_1 \times R_2 \times \dots \times R_n$ under operations:

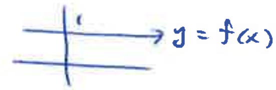
$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1+b_1, a_2+b_2, \dots, a_n+b_n)$$

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1b_1, a_2b_2, \dots, a_nb_n)$$

More examples of Rings $\mathbb{Z} \times \mathbb{Z}_3$ $\quad \mathbb{Q} \times M_2(\mathbb{R})$

Most, though not all rings will have a multiplicative identity, usually called 1, having property $1 \cdot a = a \cdot 1 = a \ \forall a \in R$
Such a ring is a ring with identity.

Ex F has mult. identity $f: \mathbb{R} \to \mathbb{R}$, $f(x) = 1$.



Ex $M_n(R)$ has mult. identity $I = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$

Ex $\mathbb{Z}_{10}$ $\quad$ Ex $5\mathbb{Z}$ has no multiplicative identity

Multiplicative inverses:

Some elements of a ring with identity will have multiplicative inverses. Such elements are called units of the ring.

Ex In $\mathbb{Z}_{10}$:

$$1 \cdot 1 = 1 \qquad 1^{-1} = 1$$
$$3 \cdot 7 = 1 \qquad 3^{-1} = 7$$
$$9 \cdot 9 = 1 \qquad 9^{-1} = 9$$

Units of $\mathbb{Z}_{10}$ are $\{1, 3, 7, 9\}$
Elements $\{0, 2, 4, 5, 6, 8\}$ are not units.

Exercise Show units of a ring form a mult. ~~addition~~ group

Units of $\mathbb{Z}_{10}$: $3^0, 3^1, 3^2, 3^3$,
$\qquad 1 \quad 3 \quad 9 \quad 7$

$\cdot$	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Thus group of units $\cong \mathbb{Z}_4$.

Now we add more structure to a ring:

Def A division ring is a ring for which every nonzero element is a unit.

Ex $\cancel{GL}(n, \mathbb{R})$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$ ...

Def A field is a commutative division ring

Ex $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$ ... we will see other examples.

Definitions

If R and S are rings, $\varphi: R \to S$ is a homomorphism if $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall\, a, b \in R$

If φ is 1-1 and onto homomorphism it is an isomorphism

$\mathrm{Ker}(\varphi) = \{a \in R \mid \varphi(a) = 0\}$.

A subset $S \subseteq R$ is a subring of R if S is also a ring under R's operations. We write $S \leq R$.

Ex $\mathbb{Z} \leq \mathbb{R}$ $\quad \mathbb{Q} \leq \mathbb{R}$ $\quad \mathbb{R} \leq \mathbb{C}$ $\quad \mathbb{Z} \leq \mathbb{C}$

How to show subset $S \subseteq R$ is a subring

1. Show S is an additive subgroup of R.
    1. closed under addition.
    2. $0 \in S$
    3. If $a \in S$ then $-a \in S$.
2. Show S is closed under multiplication.

Do This for Sec 18 # 12