14th June 2024

Definition $\boxed{1\cdot 6:}$ 2.16

(ii) A group $(G, *)$ for which the binary operation '$*$' is commutative, is called a commutative group (also called an Abelian group after N. Abel) if the binary operation '$*$' is not commutative, we call the group a non-commutative group.

(iii) A ring $(R, +, \cdot)$ is said to be a ring with unit element if there is an element 1_R different from the zero element 0_R where 0_R is the additive identity element of the

Abelian group $(R, +)$, belonging to the ring $(R, +, \cdot)$ such that for each point a of R, $a \cdot 1_R = 1_R \cdot a = a$.

Note: If 1_R exists in a ring $(R, +, \cdot)$, it is unique because $(R, \cdot)$ is then a monoid. Thus, when 1_R exists, it is called the unit element of the ring $(R, +, \cdot)$

(iv) A ring $(R, +, \cdot)$ is called a commutative ring if for all elements a, b of R, $a \cdot b = b \cdot a$ holds.

e.g. 1. The set of all even integers under additive '+' and multiplication '$\cdot$' of integers is a commutative ring but has no unit element, since the integer 1 is odd.

2. The set $\mathbb{Z}$ of all integers is a commutative ring with unit element 1, and zero element the integer 0.

(v) A non-zero element $a \neq 0_R$ in a ring $(R, +, \cdot)$ is said to be

14th June 2024.

a zero-division if there exists a non-zero element b such that $a \cdot b = 0_R$ (or, $b \cdot a = 0_R$).

e.g:

1. In the ring $M_2(\mathbb{R})$ of all 2×2 real matrices $\begin{pmatrix} \frac{1}{3} & 1 \\ \frac{1}{3} & 1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}$ are zero-divisors, since

$$\begin{pmatrix} 1/3 & 1 \\ 1/3 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 3 \\ 1/3 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

and $\begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Note: $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the zero element of the ring.

(vi) An integral domain is defined as the commutative ring having no zero-divisors.

e.g. The set $\mathbb{Z}(\sqrt{2}) = \{$all real numbers of the form $m+n\sqrt{2} : m, n$ integers$\}$ is an integral domain under addition and multiplication of real numbers.

(vii) A field is defined as a commutative ring $(F, +, \cdot)$ in which the non-zero elements form a group under '$\cdot$', that is, a ring $(F, +, \cdot)$ becomes a field if its non zero elements form an Abelian group under multiplication '$\cdot$'

e.g:

1. The set $\mathbb{Q}$ of all rational numbers, the $\mathbb{R}$ of all real numbers, and the set $\mathbb{Q}(\sqrt{2}) = \{p + q\sqrt{2} : p, q$ rationals$\}$ are fields under addition and multiplication of real numbers.

2. The set $\mathbb{Z}$ of all integers, and the set $\mathbb{Z}(\sqrt{2}) = \{m + n\sqrt{2} : m, n$ integers$\}$ are not fields, since $2 \in \mathbb{Z} \subset \mathbb{Z}(\sqrt{2})$ but has no inverse w.r.t '$\cdot$' in each of them.

Note: $\mathbb{Z}(\sqrt{2})$ is an integral domain which is not a field. Also, $\mathbb{Z}$ is an integral domain that is not a field.

(viii) A division ring (also called a skew-field) is defined as a ring

Osazuwa Emmanuel Osalotioman

$(R, +, \cdot)$ in which the non-zero elements from a group under multiplication $(\cdot)$

e.g The ring Π of linear maps $x \xmapsto{f} ax+b$, (a, b real constants) with $b = 0$ if $a = 0$ of R' into R' defines the following division ring

$$\left\{\begin{pmatrix} f & 0 \\ 0 & f \end{pmatrix} : f \in \Pi\right\}$$ where 0

denotes the function zero. But it is not a field, since $A \cdot B \neq B \cdot A$ if $A = \begin{pmatrix} h & 0 \\ 0 & h \end{pmatrix}$, $B = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}$ where $h(x) = x+2 \ \forall x \in R'$ and $p(x) = 2x \ \forall x \in R'$; (as $h \circ p \neq p \circ h$)

Definition 2.16 Contd: (ix)

A subring of a ring $(R, +, \cdot)$ is defined as a subset S of R which is a ring under induce operations from the whole ring. Thus, a subset S of a ring $(R, +, \cdot)$ is a substring if and only if,

(a) $0_R \in S$,

(b) $a-b$ belongs to S when a, b are in S, and

(c) $a \cdot b \in S$ when a, b are in S.

Note: The symbol $a-b$ means $a+(-b)$.

(*) A subfield is defined as a subset which is a field under the binary operations from the given field.

Thus, a subset A of a field $(F, +, \cdot)$ is a subfield if and only if

(a) 0_F and 1_F lie ~~are~~ in the A

(b) If x, y are in A then $x-y \in A$

(c) If x, y are in A then $x \cdot y \in A$

(d) If $x \neq 0_F$ belongs to A then $x^{-1} \in A$.

e.g 1. $\mathbb{Z}$, $\mathbb{Z}(\sqrt{2})$, $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, and R' are subgroups of the group $(\mathbb{C}, +)$ of all complex numbers w.r.t addition of complex numbers.

2. $\mathbb{Z}$, $\mathbb{Z}(\sqrt{2})$, $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$ are subrings of the ring $(R', +, \cdot)$ of all real numbers

Osazuwa Emmanuel Osalotioman

W.r.t addition and multiplic-
-ation of real numbers

3. Both Z and $Z(\sqrt{2})$ are not subfields of the real field $(R', +, \cdot)$.

4. The rational field Q and the field $Q(\sqrt{2})$ are subfields of the real field $(R', +, \cdot)$

5. The real field $(R', +, \cdot)$ is a subfield of the complex field $(\mathbb{C}, +, \cdot)$

Definition 2.17:

A subdomain of an integral domain $(D, +, \cdot)$ with unit element 1_D is defined as a subset S of D which is also an integral domain with unit element for the same operations of addition '+' and multiplication '$\cdot$'. Thus a subset is a subdomain if and only if, it is a subring that contains the unit element.

Definition 2.18:

An integral domain $(D, +, \cdot)$ with unit element 1_D is said to be an ordered domain if there are certain elements of D called the positive elements such that:

(a) The sum of two positive elements is a positive element.

(b) The product of two positive elements is a positive element.

(c) given $a \in D$, either a is a positive element or a is the zero element 0_D, or $-a$ is a positive element.

Note: The condition (c) is called the law of trichotomy.

~~The~~ Definition 2.19: In an ordered domain $(D, +, \cdot)$ with unit element 1_D, the relation, denoted "$\leq$" where $x \leq y$ means $y - x$ is a positive element or the zero element 0_D, is a linear ordering.

Osazuwa Emmanuel Osalotioman

Note: The relation denoted '$<$' is given by : $x < y$ means $y - x$ is a positive element.

Thus the positive elements $x > 0_D$ while the negative elements are the elements $y < 0_D$.

<u>Notation</u>: We shall denote an ordering domain by $(D, +, \cdot, \leq)$.

Definition 3.1: In an ordered domain $(D, +, \cdot, \leq)$, the absolute value of an element a of D, denoted $|a|$, is a if $a \geq 0_D$ (i.e. if $0_D \leq a$), and $-a$ if $a < 0_D$.

Remark 3.2: Since $-|a| \leq a \leq |a|$ and $-|b| \leq b \leq |b|$, we have on adding: $-(|a| + |b|) \leq a+b \leq |a| + |b|$. Hence 3.2.1:

$|a+b| \leq |a| + |b|$ holds

Theorem 3.3: In any ordered domain $(D, +, \cdot, \leq)$ with unit element 1_D, all squares of non-zero elements are positive.

<u>Proof</u>:

<u>Note</u>:

1. $x \cdot 0_D = 0_D \cdot x = 0_D \;\forall x \in D$

because $x \cdot 0_D = x \cdot (0_D + 0_D) = x \cdot 0_D + x \cdot 0_D$ giving $x \cdot 0_D = 0_D$, and also $0_D \cdot x = (0_D + 0_D) \cdot x = 0_D \cdot x + 0_D \cdot x$ which gives $0_D \cdot x = 0_D$, (as $a - a = 0_D \;\forall a \in D$).

2. $(a^2) = (-a) \cdot a$ because $(-a) \cdot a + a \cdot a = (-a + a) \cdot a = 0_D \cdot a = 0_D$

3. $(-a) \cdot (-a) + (-(a^2)) \underset{\text{by (2)}}{=} (-a) \cdot (-a + a) = (-a) \cdot 0_D \underset{\text{by (1)}}{=} 0_D$

so, we have

4. $(-a) \cdot (-a) = a^2$, that is, $(-a)^2 = a^2$

The proof of theorem 3.3 next lecture!)