Rings, Subrings, Zero Divisors

January 18, 2021 9:32 PM

Rings & Fields 2.2

A set R with two binary operations $+$ and $\cdot$ is called a **ring** if $\forall a,b,c \in R$

(i) $a+b \in R$

(ii) $a \cdot b \in R$

(iii) $a+(b+c) = (a+b)+c$

(iv) $a\cdot(b\cdot c) = (a\cdot b)\cdot c$

(v) $\exists\, 0 \in R$ s.t. $0+a=a$

(vi) $\exists\, 1 \in R$ s.t. $1\cdot a = a \cdot 1 = a$, $1 \neq 0$.

(vii) $a+b=b+a$

(viii) $\exists\, -a \in R$ s.t. $a+(-a)=0$ and

(ix) $a\cdot(b+c) = a\cdot b + a \cdot c$ and $(a+b)\cdot c = a\cdot c + b \cdot c$ hold.

Remark: Most texts do not require (vi).

Definition: If R is a ring and $a\cdot b = b \cdot a$ for all $a,b \in R$ then R is called a **commutative ring**.

Definition: If $a \in R$ and $\exists\, b \in R$ s.t. $a\cdot b = b\cdot a = 1$ Then a is called a **unit** or **invertible** in R and b is called the inverse of a denoted a^{-1}.

Definition: If R is a commutative ring and every non-zero element of R is invertible Then R is called a **field**.

$\mathbb{R}$

$\mathbb{C}$

Example: $\mathbb{Z}$ is a commutative ring.

The units in $\mathbb{Z}$ are $\{1,-1\}$

$2 \quad \frac{1}{2}$

Hence $\mathbb{Z}$ is not a field.

$(-1)\cdot(-1) = 1$

Lemma. 1. If R is a ring then

(i) 0_R is unique, (ii) 1_R is unique, (iii) inverses are unique.

Proof of (iii) Suppose b and c are inverses of a. Show $b=c$.

$b\cdot a = 1$ and $a\cdot b = 1$ $\quad$ $c\cdot a = 1$ and $a\cdot c = 1$.

$$\Rightarrow ab = ac$$
$$\Rightarrow b(ab) = b(ac) \Rightarrow \underset{1}{(ba)}\cdot b = \underset{1}{(ba)}\cdot c$$
$$\Rightarrow 1\cdot b = 1\cdot c$$
$$\Rightarrow b = c.$$

25

Def. Let R^* denote the set of units in R.

Example $\mathbb{Z}_6 = \{0,1,2,3,4,5,6\}$

$\mathbb{Z}_6^* = \{1,5\}$

x	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Lemma 2. R^* is closed under $\times$, i.e.,
if $a,b \in R^*$ then $a\cdot b \in R^*$.

Proof.

$$(a\cdot b)(b^{-1}a^{-1}) = (a\cdot\overset{1}{(b\cdot b^{-1})})\cdot a^{-1} = \overset{a}{(a\cdot 1)}\cdot a^{-1} = 1$$
$$(b^{-1}a^{-1})(a\cdot b) = (b^{-1}(a^{-1}\cdot a))\cdot b = b^{-1}(1)\cdot b = 1.$$

So the inverse of ab is $b^{-1}a^{-1}$ and hence $a\cdot b \in R^*$.

Subrings. Let R be a ring and $S \subset R$.
If S is a ring then S is <u>a subring</u> of R.
Example $\mathbb{Z} \subset \mathbb{R}$ so $\mathbb{Z}$ is a subring of $\mathbb{R}$.

Lemma 3 (Subring test). Let R be a ring and $S \subset R$.
If (1) S is closed under $+$ $\quad$ (2) S is closed under $\times$.
(3) $0_R \in S$. $\quad$ (4) S has negatives.

then S is a ring.

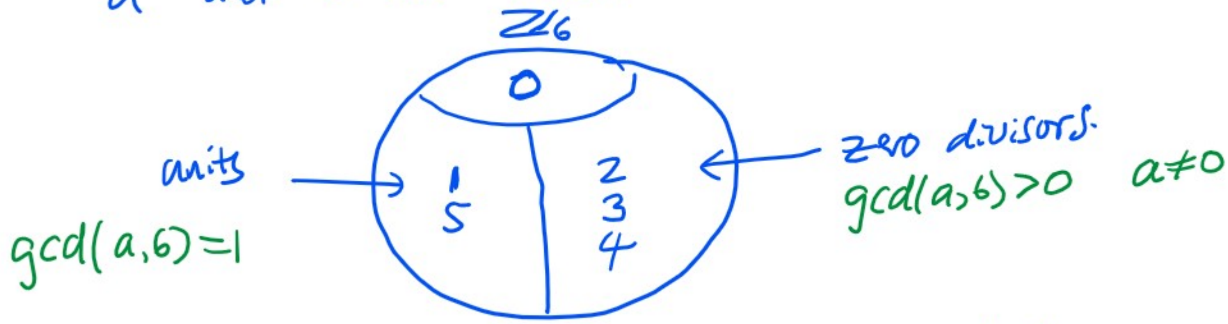
Why don't we have to check $\underset{R}{x} +_R \underset{R}{y} = \underset{R}{y} +_R \underset{R}{x}$ in S?
Because $+$ in R is comm.

Example. The even integers $2\mathbb{Z} = \{0, \pm 2, \pm 4, \dots\}$
(1) even + even = even (2) even × even = even.
(3) 0 is even. (4) − even = even.

Exercise. Let $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$
Show that $\mathbb{Z}[i]$ is ring.
Since $\mathbb{Z}[i] \subset \underset{\text{ring.}}{\mathbb{C}}$ it suffices to show $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

In $\mathbb{Z}$ $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$.
In $\mathbb{Z}_6$ $2 \cdot 3 = 0$ and $3 \cdot 4 = 0$.

Def. If $a \cdot b = 0$ in a ring and $a \neq 0$ and $b \neq 0$ then a and b are called zero-divisors.



Lemma 4. In a ring R a unit cannot be a zero divisor.

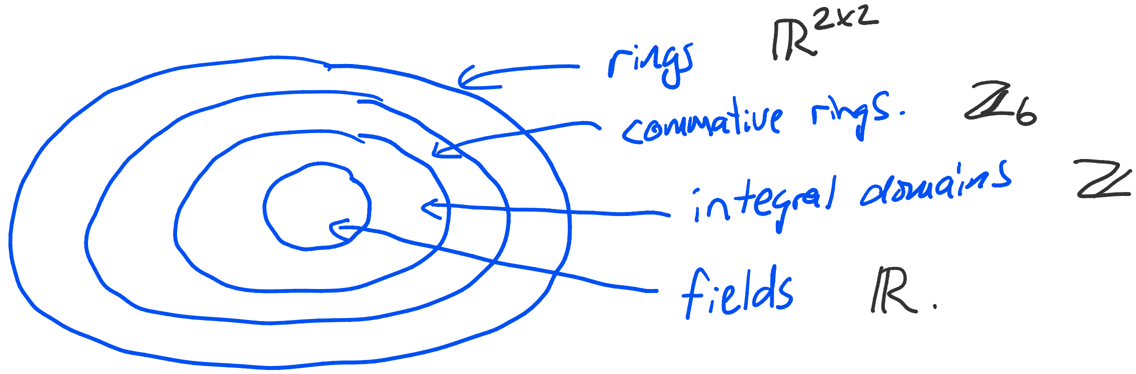
Proof. TAC Suppose u is a z.d. and a unit.
Then $\exists v \in R$, $v \neq 0$ and $\overset{\neq 0}{u} \cdot v = 0$ and $\exists w \in R$, $w \neq 0$ and $w \cdot u = 1$ $\Rightarrow$ $w(u \cdot v) = w \cdot 0 = 0$. $(w \cdot u)v = 1 \cdot v = v \neq 0$
A contradiction. □.

Corollary. In a field all non-zero elements are units.

A contradiction.

Corollary. In a field all non-zero elements are units. So a field ($\mathbb{R}$) cannot have zero divisors.

Definition. A commutative ring with no zero divisors is called an <u>integral domain</u>. E.g. $\mathbb{Z}$.



Exercise. Let $\mathbb{R}^{2\times 2} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R} \right\}$

In $\mathbb{R}^{2\times 2}$ $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 0 & b \end{bmatrix} = \underline{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}}$

zero divisors.

Question: which matrices are zero divisors?