

§ 19 Fields and integral domains

ring $R \Rightarrow$ we have the additive identity elem. 0
 $(0 + a = a = a + 0)$

but in general no multiplicative identity elem.

Ex. $R = 2\mathbb{Z} = \{\text{even integers}\}$

no number $a = 2k$ satisfies $ab = b = ba$

Def. If there is a multiplicative identity element
 (write $1 \in R$) i.e., $1 \cdot a = a = a \cdot 1$ for all $a \in R$
 we say R is a ring with unity (unital ring)

We also say 1 is the unity of R
 (not to be confused with units)

Ex. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \dots$ has the usual num. 1 as mult. id.

M_n has I_n as mult. id.

$\mathbb{Z}G$ has $1 \cdot e$ as mult. id.

What kind of rings are closer to usual number systems?

- commutative rings : mult. is comm. $a \cdot b = b \cdot a$

Ex. $\mathbb{Z}, \mathbb{Q}, \mathbb{Z}_m, \dots$; Non-ex. M_n $n \geq 2$, $\mathbb{Z}G$ $\downarrow$ non-comm.

- integral domains : comm. rings such that $1 \neq 0$
 $a \neq 0 \neq b \Rightarrow ab \neq 0$ (with mult. id. 1)

Ex. $\mathbb{Z}, \mathbb{Q}, \dots$ Non-ex. $\mathbb{Z}_6$ $[2] \cdot [3] = [6] = [0]$

- fields : comm. rings with mult. id. 1

such that $1 \neq 0$, $a \neq 0 \Rightarrow \exists b : ab = 1$
 write $b = a^{-1}$

Ex. $\mathbb{Q}, \mathbb{R}, \dots$ Non-ex. $\mathbb{Z}$

When R is a ring, $a, b \in R$ are s.t. $a \neq 0 \neq b$ but
 $ab = 0$, we say a, b are 0 divisors

So integral dom. $\equiv$ comm. ring with mult. id. $1 \neq 0$
 and without 0 divisors

a unit of ring with mult. id. : $u \in R$ s.t. $\exists u^{-1}$
Structure of $\mathbb{Z}_m$

We have a ring isom. $\mathbb{Z}_{ab} \rightarrow \mathbb{Z}_a \times \mathbb{Z}_b$
 $\phi([k]) \mapsto ([k], [k])$
if a and b have no common divisors

What are the 0-divisors in $\mathbb{Z}_m$?

$a \neq 0 \neq b$ and $ab = 0$ in $\mathbb{Z}_m$ means
 $m \nmid a$, $m \nmid b$ and $m \mid ab$

$\Rightarrow$ both a and b have divisors of m
(cf. Thm 19.3)

to find such a and b , m should have more
than one divisors (i.e., not prime)

$\Rightarrow \mathbb{Z}_m$ is $\begin{cases} \cdot \text{ not an integ. dom. if } m \text{ is not prime} \\ \cdot \text{ an integ. dom. if } m \text{ is prime} \end{cases}$

Thm 19.11 Suppose R is a finite ring

Then R is an integ. dom. $\Leftrightarrow R$ is a field

Proof : we need to check " $\Rightarrow$ "

i.e. want $a \neq 0 \Rightarrow \exists b : ab = 1$ from R being
a finite integ. dom.

write $R = \{a_0 = 0, a_1, a_2, \dots, a_n\}$ $a_i \neq a_j$ for $i \neq j$

Step 1 $(aa_i)_{i=0}^n$ are all distinct.

$aa_i - aa_j = a \underbrace{(a_i - a_j)}_{\neq 0} \neq 0$ by integ. dom. condition

Step 2 There is some i s.t. $aa_i = 1$

R has $(n+1)$ elements, $(aa_i)_{i=0}^n$ are all distinct $\square$

Thm 19.9 R is a field $\Rightarrow R$ is an integ. dom.

Proof assuming mult. id. $1 \neq 0$

Want : $\exists a^{-1} \Rightarrow a$ is not a zero-divisor

If $ab = 0$ we get $a^{-1}ab = \begin{cases} b \\ 0 \end{cases}$

hence $b = 0$; a cannot be a zero-div. $\square$

Other related concepts / facts

- nilpotent element : $a \in R$ s.t. $a^n = 0$ for some n

Ex. $a = \begin{bmatrix} 0 & 1 & & 0 \\ & 0 & \ddots & \\ 0 & & \ddots & 1 \\ & & & 0 \end{bmatrix} \in M_n$

They behave like "infinitesimals"

$$(\lambda 1 + a)^m = \lambda^m 1 + m \lambda^{m-1} a + \dots + \binom{m}{n-1} \lambda^{m-n+1} a^{n-1}$$

if $a^2 = 0$ $f(\lambda + a) = f(\lambda) + f'(\lambda)a$

In general Taylor series exp. up to order $n-1$

- nontrivial direct products are never intes. dom.

$R_1 \times R_2$ contains $(a, 0)$, $(0, b)$

their prod. $(a, 0) \cdot (0, b) = (a \cdot 0, 0 \cdot b) = (0, 0)$

Ex. $\mathbb{Z}_{a'b'} \cong \mathbb{Z}_{a'} \times \mathbb{Z}_{b'}$ for coprime a', b'

- skew-fields : (possibly) non-commutative ring

with $\begin{cases} \text{mult. id. } 1 \neq 0 \\ \text{for any } a \neq 0 \exists b \text{ s.t. } ab = 1 = ba \end{cases}$

Ex. Quaternion $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$
 $i^2 = j^2 = k^2 = -1, ij = k = -ji$

1. The first part of the paper is devoted to the study of the properties of the function $f(x)$ defined by the equation

$$f(x) = \int_0^x \frac{1}{1+t^2} dt$$

It is well known that this function is the arctangent function, i.e. $f(x) = \arctan x$.

The second part of the paper is devoted to the study of the properties of the function $g(x)$ defined by the equation

$$g(x) = \int_0^x \frac{t}{1+t^2} dt$$

It is well known that this function is the logarithm of the square of the square root of $1+x^2$, i.e. $g(x) = \frac{1}{2} \ln(1+x^2)$.

The third part of the paper is devoted to the study of the properties of the function $h(x)$ defined by the equation

$$h(x) = \int_0^x \frac{t^2}{1+t^2} dt$$

It is well known that this function is the difference between the logarithm of the square of the square root of $1+x^2$ and the function $g(x)$, i.e. $h(x) = \frac{1}{2} \ln(1+x^2) - g(x)$.

The fourth part of the paper is devoted to the study of the properties of the function $k(x)$ defined by the equation

$$k(x) = \int_0^x \frac{t^3}{1+t^2} dt$$