April6

Monday, April 5, 2021 10:07 PM

The theory of Rings

1 binary operation $\rightsquigarrow$ 2 binary operations.

Seen a few of these

Fields $+, \times, -, \div$

$\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_p$.

Notice Something like $\mathbb{Z}$ doesn't have division.

Does have $(+, -, \times)$ + distributive law.

Rmk

- In $\mathbb{Z}$, we have notions of primes, of divisibility, of factorization & more.
- In a field, everything divides everything

Pf/ $a \neq 0$ $a | b$.

$ak = b$ w/ $k = a^{-1}b$. $\varnothing$

Spend some time with examples.

First Theme: Number Theory

(Arithmetic).

- Gaussian Integers: $i^2 = -1$

$\mathbb{Z}[i] = \{a + bi \; : \; a, b \in \mathbb{Z}\}$

Have + $(a_1+b_1 i)+(a_2+b_2 i) = (a_1+a_2) + (b_1+b_2 i)$

Have 0 $a+bi + 0+0i = a+bi$

Have × $(a_1+b_1 i)(a_2+b_2 i)$

$= a_1 a_2 + a_1 b_2 i + b_1 a_2 i + b_1 b_2 i^2$

$= (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2) i \in \mathbb{Z}[i]$

Have 1 $(1+0i)(a+bi) = a+bi$

Have −

Not ÷ check

See only divide by ±1 & ±i

Fact (Gauss)

$\mathbb{Z}[i]$ have unique factorization into irreducible elements.

- Similar example ✓

$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$

Similar to $\mathbb{Z}[i]$ but 2 main differences.

1) only divide by ±1.

2) LOSE UNIQUE FACTORIZATION.

$6 = 2 \cdot 3$

$$(1+\sqrt{-5})(1-\sqrt{-5}) = 1 - \sqrt{-5} + \sqrt{-5} - (\sqrt{-5})^2$$
$$= 1+5 = 6.$$

What's going on?

Rings give us a way to quantify & ask & answer these sorts of questions.

(Number Theory / Algebraic Number Theory)

Second Theme: Rings of Functions.

Ex
$$\mathbb{R}[x] = \{a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n : a_i \in \mathbb{R}\}.$$

I can add & subtract & multiply.

Not always divide.

Understanding this ring

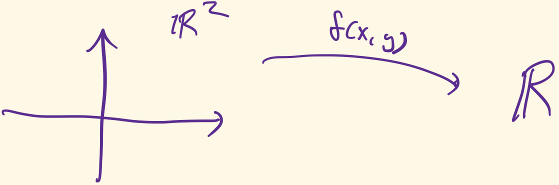
⇝ Factoring polynomials.

⇝ Look @ $\mathbb{Q}[x]$ ← Zeros. of polynomials

(Galois Theory ⇝ No quintic formula).

Ex
$$\mathbb{R}[x,y] : \{\textstyle\sum a_{ij} x^i y^j : a_{ij} \in \mathbb{R}\}$$ ← Maybe related to geometry?

These elts give you functions



Ex X a topological space $(\mathbb{R}^2)$

$$C(X) = \{ f : X \longrightarrow \mathbb{R} : f \text{ is continuous} \}.$$

$f, g \in C(X)$.

$$(f+g)(x) = f(x) + g(x)$$

$$(f \cdot g)(x) = f(x)\,g(x).$$

Have 1

$f(x) = 1 \quad \forall x$

Have 0

$f(x) = 0 \quad \forall x$

Algebraic Geometry uses this ring to build a dictionary

$$\begin{pmatrix} \text{Algebra of} \\ C(X) \end{pmatrix} \longleftrightarrow \begin{pmatrix} \text{Geometry of} \\ X \end{pmatrix}$$

tools of abstract algebra

Tools of geometry.

Third Theme: Linear Algebra.

Matrix Rings

$$M_n(\mathbb{R}) = \{ n \times n \text{ matrices over } \mathbb{R} \}.$$

Has +

$M+N$ coordinatewise $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix}$

$$= \begin{pmatrix} a+\hat{a} & b+\hat{b} \\ c+\hat{c} & d+\hat{d} \end{pmatrix}$$

MN matrix multiplication

Check Distributive Law Holds.

Have $0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & & \\ 0 & \cdots & 0 \end{pmatrix}$ (additive identity)

Have $1 = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ 0 & \cdots & 1 \end{pmatrix}$ (multiplicative identity)

$MN \neq NM$ in general

$(M+N = N+M)$.

Linear Algebra

$M_n(\mathbb{R}) \longleftrightarrow$ Linear maps $\mathbb{R}^n \longrightarrow \mathbb{R}^n$

$\Uparrow$

algebraic

Fourth Theme (Cryptography).

- $\mathbb{Z}/n\mathbb{Z}$ ring w/ + & ×.

  Crucial in cryptography.

With these as motivating examples, we define...

Def^n (Impt)

A ring R is a set, together with two binary operation $+$ & $\times$ called addition and multiplication respectively satisfying...

i) $(R,+)$ is an abelian group.

ii) $\times$ is associative. $\forall\ a,b,c \in R$,

$$a\times(b\times c) = (a\times b)\times c$$

iii) The distributive law holds. $\forall\ a,b,c \in R$

$$a\times(b+c) = (a\times b)+(a\times c)$$

$$(b+c)\times a = (b\times a)+(c\times a)$$

Remark

1) $\times$ need not be commutative.
2) $\times$ need not have inverses.
3) $\times$ need not have an identity.

Def^n

Let R be a ring.

1) If $a\times b = b\times a$ for all $a,b \in R$, we call R commutative.

2) If R has a multiplicative identity, that is, $\exists\ 1 \in R$ s.t. $\forall\ a \in R$

$$1 \times a = a \times 1 = a$$

the R is called unital.

(R has 1. R has an identity)..

3) A unital ring s.t. for all $a \in R$, $\exists$ $a^{-1} \in R$ s.t. $a \times a^{-1} = a^{-1} \times a = 1$ is called a division ring.

4) A commutative unital division ring is called a field.

Notation

- write ab instead of $a \times b$.
- Write 0 for the additive identity of R

$$0 + a = a + 0 = a$$

- Write $-a$ for additive inverse of a

$$a + (-a) = 0.$$

Proof of concept

If $1 \in R$, distributive law $\Longrightarrow$ $+$ commutative.

Pf/ $(1+1)(a+b) = 1(a+b) + 1(a+b) = a+b+a+b$

$\shortparallel$

$(1+1)(a+b) = (1+1)a + (1+1)b = a+a+b+b$

Subtract b from right & a from left

$b + a = a + b$ ✓

Examples

1) Trivial Rings R = abelian group
$ab = 0 \quad \forall \; a, b \in R.$

Check nonunital commutative ring.

1a) $R = \{0\} \leftarrow$ zero ring.
unital
$1 = 0$

Rmk Only ring w/ $1 = 0$. Proof later.

2) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ rings. $\leftarrow$

3) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$
Axioms bc hold for $\mathbb{Z}$.

commutative
unital

4) Rings of functions. R be any ring. X a set
$A = \mathrm{Maps}(X, R) = \{ f : X \longrightarrow R \}$ is a ring.

Exercise
$(f+g)(x) = f(x) + g(x)$
$(fg)(x) = f(x)g(x)$

R commutitive $\Longrightarrow$ A is
R unital $\Longrightarrow$ A is $(1(x) = 1_A)$

Distributive Law.

$f(g+h) = f \cdot g + h \cdot g. \quad (*)$

2 functions are = if they are = when evaluated at each point

$$(F = G \iff F(x) = G(x) \quad \forall\, x \in X).$$

$$
\begin{aligned}
(f(g+h))(x) &= f(x)(g(x)+h(x)) \\
&= f(x)g(x) + f(x)h(x) \qquad (R \text{ a ring}) \\
&= (fg + fh)(x) \qquad \varnothing
\end{aligned}
$$

Example of a division ring that is not a field.

Hamilton's Quaternions

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}.$$

Addition: Componentwise

$$(a + bi + cj + dk) + (\hat{a} + \hat{b}i + \hat{c}j + \hat{d}k)$$

$$= (a+\hat{a}) + (b+\hat{b})i + (c+\hat{c})j + (d+\hat{d})k.$$

$$(\mathbb{H}, +) \simeq (\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}, +)$$

$$(a + bi + cj + dk) \longmapsto (a, b, c, d)$$

Multiplication is defined by rules in Q_8

$i^2 = j^2 = k^2 = -1$

$ij = -ji = k$ ←

$jk = -kj = i$ ←

$ki = -ik = j$

$$\begin{aligned}(1+2j)(i+3k) &= 1i + 3k + 2ji + 6jk \\ &= i + 3k - 2k + 6i \\ &= 7i - k.\end{aligned}$$

Exercise Show this is a ring.

$$(a+bi+cj+dk)^{-1} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$$

Example of a division ring but
$ij \neq ji$ not a field.

Examples of nonunital rings

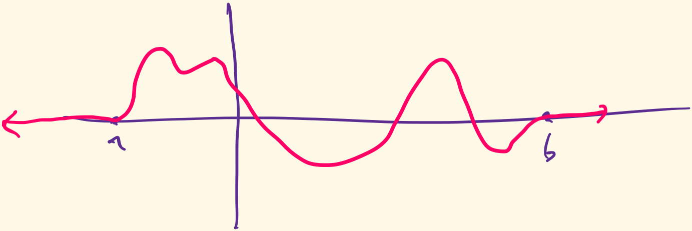
1) $(2\mathbb{Z}, +, \times)$ even #s No identity.

2) Analytic Geometry

Compactly Supported

$f:\mathbb{R}\longrightarrow\mathbb{R}$ s.t. $\exists\ [a,b]$

where $f(x)=0$ outside of $[a,b]$.



Non unital by $1(x)=1$ is mult identity
& not compactly supported.

First Properties of Rings

Prop R any ring. $a, b \in R$.

1) $0 \cdot a = a \cdot 0 = 0$
2) $(-a)b = a(-b) = -(ab)$
3) $(-a)(-b) = ab$
4) If $1 \in R$ then $-a = (-1)a$.

Proof Exercise.

I'll do (1). $0 = 0 + 0$ bc additive identity.

$$\Longrightarrow \quad 0 \cdot a = (0+0)a$$
$$= 0a + 0a \qquad \text{dist}$$

subtract $0 \cdot a$ from both sides.

$$0 = 0 \cdot a - 0 \cdot a = 0 \cdot a$$ ✓

Corollary Let R be a ring w/ $1 = 0$

Then $R = 0$.

Pf $a = a \cdot 1 = a \cdot 0 = 0$

So $a = 0$ any $a \in R$

Important Elements of Rings

Example $R = \mathbb{Z}/12\mathbb{Z}$.

1) $\overline{3}, \overline{4} \neq 0$. But $\overline{3} \cdot \overline{4} = \overline{12} = 0$

Can have $ab = 0$ $a, b \neq 0$

2) $\bar{n} \in \mathbb{Z}/12\mathbb{Z}$. $\exists\ \bar{m}$ s.t. $\bar{n}\bar{m} = 1$

$\iff \gcd(n, 12) = 1$ (Extended Euclidean Alg).

Can have $ab = 1$ w/ $a, b \neq 1$.

Def^n Let R be a ring $a \in R$.

1) a is a zero divisor if $a \neq 0$ &

$\exists\ b \neq 0$ w/ $ab = 0$.

2) Let $R \ni 1 \neq 0$.

a is a unit if $\exists\ b$ s.t. $ab = 1$.

The set of units in R is denoted

$R^\times$.

Exercise

- $R^\times$ is a group under $\times$.
- R a ring w/ $1 \neq 0$. $a \in R$
  a zero divisor. Then $a \notin R^\times$. ←

Rmk

A field is a commutative unital ring w/ $1 \neq 0$

& $F^\times = F \setminus \{0\}$. ←

Examples

1) $\mathbb{Z}$ has no zero divisors.

$\mathbb{Z}^\times = \{\pm 1\}$.

2) $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \mid \gcd(a, n) = 1\}$

Claim If $\bar{a} \notin (\mathbb{Z}/n\mathbb{Z})^\times \implies \bar{a}$ is a zero divisor.

Pf/ $g = \gcd(a,n) > 1$

Let $b = \frac{n}{g}$

$ab = a\frac{n}{g} = \frac{a}{g}\cdot n$ divisible by n

hence $\overline{ab} = 0$.

$0 < b < n$ bc $g > 1$ ∅

Corollary

$\mathbb{Z}/n\mathbb{Z}$ a field $\iff$ n is prime.

Pf/ $\implies$ A field has no zero divisors

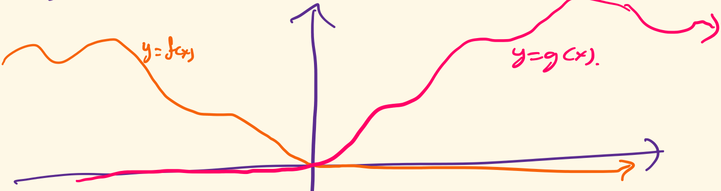
So all nonzero elts are units

hence prime to n. ∅

Example

$R = Map(\mathbb{R},\mathbb{R}) = \{ f : \mathbb{R} \longrightarrow \mathbb{R} \}$.

Has zero divisors



$f(x)=0 \quad \forall\ x \geq 0$ $\longrightarrow$ $(fg)(x) = f(x)g(x)$

$g(x)=0 \quad \forall\ x \leq 0$ $\qquad = 0 \quad \forall x$

$\Rightarrow fg = 0.$

What is $R^\times$?

Claim $f \in R^\times \Longleftrightarrow f(x) \neq 0 \quad \forall\ x.$

Pf/ Suppose $\exists\ g$ s.t. $(fg)(x) = 1 \quad \forall\ x$

$\Rightarrow$ Then $f(x)g(x) = 1 \quad \forall x$ so $f(x) \neq 0.$

$\Leftarrow$ Define $g(x) = \frac{1}{f(x)} \quad \forall\ x$

Then $(fg)(x) = f(x) \cdot \frac{1}{f(x)} = 1 \quad \forall\ x.$

Like $\mathbb{Z}/n\mathbb{Z}$

All elts of $R = \mathrm{Map}(\mathbb{R}, \mathbb{R})$ are either zero divisors or units.

Pf/ $f(x)$ not a unit. Define

$$g(x) = \begin{cases} 0 & f(x) \neq 0 \\ 1 & \text{else}. \end{cases}$$

$f(x) = 0$ @ some $x \Rightarrow g \not\equiv 0.$

so $fg = 0$ & f zero div. $\cancel{\infty}$