MATH 2022 Linear and Abstract Algebra

LECTURE 02 Wednesday 26/02/2020

Fields & other common arithmetics

① Recall

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\},$$

the arithmetic of natural numbers,

with $+$, $\times$.

— lacks negatives, so we can't always subtract.

e.g. $4 - 2 = 2 \in \mathbb{N}$, but $2 - 4 = -2 \notin \mathbb{N}$.

(2) Deficiency of $\mathbb{N}$ resolved by forming

$$\mathbb{Z} = \{ 0, \pm 1, \pm 2, \pm 3, \dots \},$$

the arithmetic of integers, with $+, \times, -$.

— lacks reciprocals (multiplicative inverses)

so we can't always divide.

e.g. $4 \div 2 = \frac{4}{2} = 2 \in \mathbb{Z}$,

but $2 \div 4 = \frac{2}{4} = \frac{1}{2} \notin \mathbb{Z}$

③ Deficiency of $\mathbb{Z}$ resolved by forming

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z} \,,\; b \neq 0 \right\},$$

the arithmetic of rational numbers,

with $+$, $\times$, $-$, $\div$, which forms a field (see below).

— but convergent sequences may not converge to rationals !!

e.g. $\sqrt{2} = 1.41421356237\ldots \notin \mathbb{Q}$

(known to the Greeks)

④ Deficiency of $\mathbb{Q}$ resolved by "completion":

$\mathbb{R} = \{$ real numbers with decimal expansions $\}$,

the arithmetic of real numbers,

with $+, \times, -, \div$, again forming a field

(see below).

- now complete: all convergent sequences converge.

- but not all polynomial equations have solutions

e.g. $\boxed{x^2 + 1 = 0}$ has no solution, i.e. $\sqrt{-1} \notin \mathbb{R}$.

5 Deficiency of $\mathbb{R}$ resolved by forming

$$\mathbb{C} = \{ a + bi \mid a, b \in \mathbb{R} \}$$

where $i = \sqrt{-1}$ (root of equation $x^2 + 1 = 0$),

which miraculously forms a field (see below),

in which all nonconstant polynomials have roots

Fundamental Theorem of Algebra

Consequence: all square matrices over $\mathbb{R}$ or $\mathbb{C}$ have eigenvalues (see later)

6 Modular arithmetic

Let $n \in \mathbb{Z}^+$. Put $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$,

the set of remainders after division by n.

e.g. $\mathbb{Z}_1 = \{0\}$, $\mathbb{Z}_2 = \{0, 1\}$, $\mathbb{Z}_3 = \{0, 1, 2\}$,

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$, $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

We can perform modular arithmetic on $\mathbb{Z}_n$:

> do arithmetic in $\mathbb{Z}$, but finish off by taking remainders after division by n.

e.g. $\mathbb{Z}_3 = \{0, 1, 2\}$ with tables

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

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

e.g. $\mathbb{Z}_3 = \{0,1,2\}$ with tables

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

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_4 = \{0,1,2,3\}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

no multiplicative inverse of 2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Example : Today is Wednesday.

What day will it be after 3^{100} days have elapsed?

Solution :

$$3^{100} = (3^3)^{33} \times 3 = (27)^{33} \times 3$$

$$= (-1)^{33} \times 3 \qquad (\text{mod } 7)$$

$27 = 21 + 6 = 3(7) + 6$

has remainder 6 after dividing by 7

$6 = -1$

in $\mathbb{Z}_7$

$\underline{\text{Example}}$: Today is Wednesday.

What day will it be after 3^{100} days have elapsed?

$\underline{\text{Solution}}$:

$$3^{100} = (3^3)^{33} \times 3 = (27)^{33} \times 3$$

$$= (-1)^{33} \times 3 \pmod 7$$

$$= -1 \times 3 = -3$$

$$= 4 \pmod 7$$

So it will be $\underline{\underline{\text{Sunday}}}$ (4 days after Wednesday).

Example: Presently it is nearly 5 pm on Wednesday. What time and day will it be after 3^{100} hours have elapsed?

Solution: First work in $\mathbb{Z}_{24}$:

$$3^{100} = (3^3)^{33} \times 3 = (27)^{33} \times 3 = 3^{33} \times 3 \pmod{24}$$

$$= (3^3)^{11} \times 3 = (27)^{11} \times 3 = 3^{11} \times 3 \pmod{24}$$

$$= 3^{12} = (3^3)^4 = (27)^4 = 3^4 \pmod{24}$$

$$= 81 = 9 \pmod{24}.$$

Hence the time will be nearly 2 am (9 hours after 5 pm).

The number of days elapsed will be

$$\frac{3^{100}-9}{24} \equiv \frac{4-2}{3} \pmod 7$$

(using earlier calculation)

$$\equiv \frac{2}{3} \equiv \frac{9}{3} \pmod 7$$

$$\equiv 3.$$

Hence the time and day will be 2 am on a Sunday

(3 days after Wednesday plus 9 hours after 5 pm).

Division by nonzero elements in $\mathbb{Z}_7$

turns out to be sensible !!

arithmetic forms a <u>field</u>

well behaved algebraic operations

Working towards a definition of a field:

In all examples so far, $+$ and $\times$ have been associative, that is,

$$a+(b+c) = (a+b)+c \quad , \quad a(bc) = (ab)c$$

bracketing does not alter the outcome

and commutative, that is,

$$a+b = b+a \quad , \quad ab = ba$$

order does not matter

In all examples there has been a zero element 0,

$$a + 0 = 0 + a = a \quad \text{for all } a$$

behaving as an additive identity element

and in all examples, except $\mathbb{N}$, there are negatives, that is,

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

which behave as additive inverses.

In all examples, multiplication **distributes over** $+$,

$$(a+b)c = ac + bc$$

we may expand brackets as usual.

In all examples, there is a **multiplicative identity element** 1,

$$1a = a1 = a \quad \text{for all } a.$$

Note also that $1 \neq 0$ in all of these examples.

A **field** is an arithmetic with all of these properties plus one more:

$\boxed{\text{all nonzero elements have multiplicative inverses}}$

that is, if $a \neq 0$ then a^{-1} exists such that

$$\boxed{a a^{-1} = a^{-1} a = 1}$$

In our examples so far

$\boxed{\mathbb{Q},\ \mathbb{R},\ \mathbb{C} \text{ are fields.}}$

In our examples so far

$\boxed{\mathbb{Q},\ \mathbb{R},\ \mathbb{C} \text{ are fields.}}$

If $a+bi \neq 0$ then $a \neq 0$ or $b \neq 0$, so that

$$(a+bi)^{-1} = \frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)}$$

$$= \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} + \left(\frac{-b}{a^2+b^2}\right)i$$

e.g. $\dfrac{1}{2+3i} = \dfrac{2-3i}{(2+3i)(2-3i)} = \dfrac{2-3i}{4+9}$

$= \dfrac{2-3i}{13} = \dfrac{2}{13} + \left(-\dfrac{3}{13}\right) i$

$$\boxed{\begin{array}{l}\underline{\text{Theorem}} \text{ (not obvious):} \\ \quad \mathbb{Z}_n \text{ is a field iff } n \text{ is a prime.}\end{array}}$$

e.g. $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{13}$ are fields,

but $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_8$, $\mathbb{Z}_{12}$, $\mathbb{Z}_{30}$ are not.

Formally, using axioms:

$(F, +, \cdot)$ is a field if F has at least two elements such that

(1) $(\forall a, b, c \in F)$ $(a+b)+c = a+(b+c)$

"for all"

and $(ab)c = a(bc)$

(associativity)

(2) $(\forall a, b \in F)$ $a+b = b+a$ and $ab = ba$

(commutativity)

"there exists"

(3) $(\exists\, 0, 1 \in F)(\forall a \in F)\quad a+0 = a = a1$

(existence of additive & multiplicative identity elements)

(4) $(\forall a \in F)(\exists\, b \in F)\quad a+b = 0$

(existence of negatives and we write $b = -a$)

(5) $(\forall a, b, c \in F)\quad (a+b)c = ac + bc$

(distributivity)

(6) $(\forall a \in F, a \neq 0)(\exists\, c \in F)\quad ac = 1$

(existence of multiplicative inverses and we write $c = a^{-1}$)