Alg-4

HW (Due 02/04/2021)

1. $b|g$ and $b|h \Rightarrow b|mg+nh$ for $b \in \mathbb{Z}$ & $g, h, m, n \in \mathbb{Z}$.

2 For p prime & $[x]_p \neq [0]_p$, Prove that there is $[y]_p \in \mathbb{Z}/p\mathbb{Z}$ s.t.

$$\underbrace{[x]_p [y]_p}_{\text{product in } \mathbb{Z}/p\mathbb{Z}} = [1]_p$$

$37^{1000} = 29^{29} + r$, find r

29

$n \in \mathbb{N}$, $x \equiv y \bmod n$ means $n \mid x-y$

or $x \overset{n}{\sim} y$ (say x is congruent to y mod n)

$\Leftrightarrow n \mid x-y$.

$[x] = \{y \in \mathbb{Z} : y \overset{n}{\sim} x$ or $y \equiv x \bmod(n)\}$,

$$[x]_n = \{ y \in \mathbb{Z} : y \sim_n x \text{ or } y \equiv x \bmod n \}$$

$$= \{ nq + x , q \in \mathbb{Z} \}$$

$n \mid y - x \Rightarrow y - x = nq$ for $q \in \mathbb{Z}$

$$\mathbb{Z}/\sim_n \equiv \mathbb{Z}/n\mathbb{Z} = \{ [x]_n : x \in \mathbb{Z} \}$$

Thm. Given $n \in \mathbb{N}$, $x \in \mathbb{Z}$. $\exists$ $r \in \{0, \dots, n-1\}$ s.t. $[x]_n = [r]_n$

proof. By Euclidean Algorithm

$\exists\, q \in \mathbb{Z}$ & $0 \le r \le n-1$ s.t.

$x = nq + r$

$\Rightarrow n \mid x - r \Rightarrow [x]_n = [r]_n$

$n = 12$ $\quad \mathbb{Z}/12\mathbb{Z} = \{ [x]_{12} : x \in \mathbb{Z} \}$

$$= \{ [0]_{12}, [1], \dots, [11]_{12} \}$$

Clock arithmetic

$$= \{ 0, 1, \dots 11 \}$$

Ex $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\sim_n = \{ [a]_n : a \in \mathbb{Z} \}$

$$= \{ [r]_n : 0 \le r \le n-1 \}$$

$$= \{ [r]_n : 0 \le r \le n-1 \}$$

$$= \{ 0, 1, 2, \ldots n-1 \}$$

If there is confusion, simply write $\mathbb{Z}/n\mathbb{Z} = \{ [0], [1], \ldots [n-1] \}$

$n \in \mathbb{Z}$, $d > 1$ integer

$$n = c_k d^k + c_{k-1} d^{k-1} + \cdots + c_2 d^2 + c_1 d + c_0$$

$$0 \le c_j \le d-1$$

Notation $= (c_k c_{k-1} \cdots c_2 c_1 c_0)_d$, $c_0, \ldots c_k$ are called d-digits.

d-ary expansion.

$d=2$ binary
$d=3$ ternary
$d=10$ decimal

$$738 = 7 \cdot 10^2 + 3 \cdot 10 + 8$$

$$= (c_k c_{k-1} \cdots c_2 c_1 c_0)_2 = c_0 + c_1 2 + c_2 2^2 + \cdots + c_k 2^k$$

$0 \le c_j \le 1$, c_j integer

Have seen $x \underset{n}{\sim} a$, $y \underset{n}{\sim} b$

Then (1) $x+y \underset{n}{\sim} a+b$

(2) $xy \underset{n}{\sim} ab$

Thm $\mathbb{Z}/n\mathbb{Z} = \{[x]_n : x \in \mathbb{Z}\}$

Define $[a]_n \oplus_n [b]_n = [a+b]_n$ — sum

$[a]_n \otimes_n [b]_n = [ab]_n$ for $a, b \in \mathbb{Z}$.

— product

Then sum & product are well defined and satisfy the following

(1) $[a]_n \oplus_n [b]_n = [b]_n \oplus_n [a]_n$, $[a]_n \otimes_n [b]_n = [b]_n \otimes_n [a]_n$

commutative law

(2) $[a]_n \oplus_n ([b]_n \oplus_n [c]_n) = ([a]_n \oplus_n [b]_n) \oplus_n [c]_n$

$[a]_n \otimes_n ([b]_n \otimes_n [c]_n) = ([a]_n \otimes_n [b]_n) \otimes_n [c]_n$

associative law

(3) $[a]_n \oplus_n [0]_n = [a]_n = [0]_n \oplus_n [a]_n$

$[a]_n \otimes_n [1]_n = [a]_n = [1]_n \otimes_n [a]_n$

(4) for each $[x]_n$, there $[y]_n$ s.t. $[x]_n \oplus_n [y]_n = [0]_n$

$[0]_n$ is called

$[1]_n$ is called a

$[0]_n$ is called an additive identity

$=$ on

called a multiplicative identity

Will see later that these identities are unique

Sketch. sum & product are well defined: $[a]_n = [x]_n$

$[b]_n = [y]_n$

then $[a]_n \oplus_n [b]_n = [x]_n \oplus_n [y]_n$

$[a]_n \otimes_n [b]_n = [x]_n \otimes_n [y]_n$

$[a]_n = [x]_n \Rightarrow a \sim_n x \Rightarrow n \mid a - x$

$a - x = q_1 n$

Similarly $b - y = q_2 n$

$a + b = x + q_1 n + y + q_2 n$

$= x + y + (q_1 + q_2) n$

$ab = (x + q_1 n)(y + q_2 n)$

$= xy + (xq_2 + yq_1 + q_1 q_2 n) n$

$\Rightarrow a+b \underset{n}{\sim} x+y \;\wedge\; ab \underset{n}{\sim} xy$

$\Rightarrow [a+b]_n = [x+y]_n \;\wedge\; [ab]_n = [xy]_n$

$[a]_n \oplus_n [b]_n$ $\quad$ $[x]_n \oplus_n [y]_n$ $\quad$ similarly

---

⑤ $[x]_n \otimes ([a]_n \oplus [b]_n)$

$= [x]_n \otimes_n [a]_n \oplus_n [x]_n \otimes_n [b]_n$

distributive law.

Not always true that for each $[x]_n \in \mathbb{Z}/n\mathbb{Z}$ there is $[y]_n \in \mathbb{Z}/n\mathbb{Z}$ s.t. $[x]_n \otimes [y]_n = [1]_n$

Ex. $[3]_{12} \otimes_{12} [4]_{12} = [0]_{12}$

$[1]_{12}$ $\quad$ false

Euclid's lemma, p is prime

$a \mid b$ or $b \mid b$

Euclid's Lemma

$p \mid ab, \Rightarrow p \mid a$ or $p \mid b$

$\forall\ a, b \in \mathbb{Z}$.

Proof Assume $p \mid ab$. If $p \mid a$, then done. Suppose not. $p \nmid a$

then $(p, a) = 1$ as if $d = \gcd(a, p)$

$\gcd(p, a)$

then $d \mid p$

$d = 1$ or $d = p$ ✗

$1 = rp + sa$ for some $r, s \in \mathbb{Z}$.

Now $b = b1 = b(rp + sa)$

$= brp + sab$

$= brp + sgp$ as $ab = gp$ for some $g \in \mathbb{Z}$.

$= (br + sg)p$

$\Rightarrow p \mid b$

This Lemma is false if p is not prime.

not prime.

$\exists\, a, b \in \mathbb{Z}$, m composite s.t

$m \mid ab$ but $m \nmid a$ and $m \nmid b$

$m = 4$, $a = 2 = b$

$4 \mid 2 \cdot 2$ but $4 \nmid 2 \wedge 4 \nmid 2$

Find the last digit of 3^{1000}.

Sol. $3^{1000} = \sum_{j=0}^{k} c_j 10^j$

$= c_0 + 10\left(\sum_{j=1}^{k} c_j 10^{j-1}\right)$

$3^2 = 9$. $3^3 = 27 = 2 \cdot 10 + 7$

$3^3 = 7 \bmod 10$

$3^6 = (3^3)^2 = 7^2 \bmod 10$

$= 9 \bmod 10$

$3^{12} = 81 \bmod 10$

$= 1 \bmod 10$

$x \sim a$

$y \sim b$

$xy \sim ab$

$3^{24} = 1 \mod 10$

$3^{48} = 1 \mod 10$

$3^{96} = 1 \mod$

$3^{192} = 1$ - -

$3^{384} = 1 \mod$

$3^{768} = 1 \mod 10$

$3^{1000} = 3^{768} \cdot 3^{232} = 1 \mod 10$

last digit of 3^{1000} is 1.

Ex remainder of 37^{1000} when devided 29.

$37 = 8 \mod 29$

$37^2 = 64 \mod 29$

$= 6 \mod 29$

$37^4 = 36 \mod 29$

$= 7 \mod 29$

$8 \ldots a \mod 29$

$29 \overline{)1400}$ (3, 29, 110, 87, 23, 23, 169)

$39^8 = 49 \bmod 29$
$= 20 \bmod 29$

$39^{16} = 400 \bmod 29$
$= 23 \bmod 29$

$39^{32} = 529 \bmod 29$
$= 7 \bmod 29$

Please complete it.

1.1 Algebraic structure is Group. (Galois)

Ex $(\mathbb{Z}, +)$ has the following properties

1 $-(a+b) + c = a + (b+c)$, sum is associative

2 $a + 0 = 0 + a = a$ for each $a \in \mathbb{Z}$
0 is called the additive identity

3 for each $a \in \mathbb{Z}$, $\exists\, b \in \mathbb{Z}$ s.t.
$a + b = 0 = b + a$. b is called
the additive inverse of a &
is denoted by $b = -a$, negative
of a

4) $a + b = b + a$ — commutative law

4) $a+b=b+a$ — commutative law

$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by

$+(a,b) \equiv a+b$

Ex $\mathbb{F} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, there is a map

$+ \cdot \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ given by

$+(a,b) = a+b$, called the sum of a & b. It satisfies:

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

associative law

(2) There $0 \in \mathbb{F}$ s.t. $a+0=a=0+a$

↑ additive id.

(3) for each $a \in \mathbb{F}$, there is $b \in \mathbb{F}$ s.t. $a+b=0=b+a$. b is called the additive inverse of a & is denoted by $b=-a$, called the negative of a

(4) $a+b=b+a$ $\forall\, a,b \in \mathbb{F}$

commutative law

Ex $\mathbb{F}^* = \mathbb{F}-0 = \mathbb{F}-\{0\}$

$\{\mathbb{F} : a \neq 0\}$

Ex $\mathbb{F}^* = \mathbb{F} - 0 = \{a \in \mathbb{F} : a \neq 0\}$

where $\mathbb{F} = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$

$\mathbb{R}$: reals, $\mathbb{C}$: complex #s

$\cdot : \mathbb{F}^* \times \mathbb{F}^* \to \mathbb{F}^*$

by $\cdot(a,b) = ab$, product of a, b. It satisfies

(1) $a(bc) = (ab)c$ assoc

(2) $a1 = a = 1a$ $\forall a \in \mathbb{F}^*$, 1 is (the) multiplicative unit or identity of $\mathbb{F}^*$.

(3) For each $a \in \mathbb{F}^*$, there $b \in \mathbb{F}^*$ s.t. $ab = 1 = ba$.

b is called (the) multiplicative inverse of a & is denoted by $b = a^{-1} = \frac{1}{a}$. It is called the reciprocal of a

Ex $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots n-1\}$

$i + j \in \mathbb{Z}/n\mathbb{Z}$

1) $(i+j)+k = i+(j+k)$

2) $i+0 = 0+i = i$

3) for each $i \in \mathbb{Z}/m\mathbb{Z}$

there is $j \in \mathbb{Z}/m\mathbb{Z}$

s.t. $i+j = 0 \Rightarrow j = -i$

Ex $\mathbb{Z}/12\mathbb{Z} = \{0, 1, 2, \dots, 11\}$

-11 in $\mathbb{Z}/12\mathbb{Z}$ is 1. -2 is 10

$4 \cdot 3 = 0 = 6 \cdot 2 = 2 \cdot 6$

$\mathbb{F} = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$

$GL(n, \mathbb{F}) = \{ A \in M_{n\times n}(\mathbb{F}) : AB = I_n = BA \}$

$B = A^{-1} \in$ Inv A for some $B \in M_{n\times n}(\mathbb{F})$

I_n – identity matrix

$(A)_{ij} = a_{ij}$ – entry in ith row & jth column

$(AB)_{ij} = \sum_{k=1}^{n} (A)_{ik} (B)_{kj}$ / product of A&B

$AB \neq BA$

- $GL(n, \mathbb{F}) \times GL(n, \mathbb{F}) \to GL(n, \mathbb{F})$
- $(A, B) = AB$

Thm $A, B \in M_{n\times n}(\mathbb{F})$ invertible

$\Rightarrow$ AB is invertible &

$(AB)^{-1} = B^{-1}A^{-1}$

Proof A is invertible $\Rightarrow$

$AS = SA = I_n$ for

some $S \in M_{n\times n}(\mathbb{F})$

B is invertible $\Rightarrow$ $T \in M_{n\times n}(\mathbb{F})$

s.t. $BT = TB = I_n$

$$(AB)(TS) = A(BT)S = A(I_n)S = A(I_nS) = AS = I_n$$

$$(TS)(AB) = T(SA)B = T(I_n)B = (TI_n)B$$

$= TB$

$= I_n$

$$(AB)^{-1} = TS = B^{-1}A^{-1}$$

Back to $GL(n, \mathbb{F})$

(1) $A(BC) = (AB)C$ associative

(2) $AI_n = I_n A = A$.

(3) For each $A \in GL(n, \mathbb{F})$, there $B \in GL(n, \mathbb{F})$ s.t. $AB = I_n = BA$.

There are some $A, B \in GL(n, \mathbb{F})$ s.t $AB \neq BA$ · for some n.

$n=2$, $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ or $\mathbb{Q}$

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad B = A^t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

A, B are invertible

$AB \neq BA$.

$$AB = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

$$BA = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

Def $\phi \neq G$, $\cdot : G \times G \to G$, $\cdot(a,b) = ab$, satisfying

(1) $a(bc) = (ab)c$ — associative law

(2) $\exists\, e \in G$ s.t. $ae = ea = a$ for each $a \in G$

(3) For each $a \in G$, there is $b \in G$ s.t.

$$ab = e = ba.$$

The pair $(G, \cdot)$ is called a group or simply G is a group when $\cdot$ is understood.

Thm (1) e in (2) is unique

(2) b in (3) is unique.

Proof (1) Suppose there is another $e' \in G$ s.t $e'a = a = ae'$ for each $a \in G$

To show $e = e'$

$e = ee'$ as e' is identity w.r.t $\cdot$

$= e'$ as e is identity. w.r.t.

(2) let $a \in G$, suppose there are $b, \& b' \in G$ s.t

$ab = ba = e$ and

$ab' = b'a = e$

To prove $b = b'$

$b' = b'e = b'(ab) = (b'a)b$ by associative law as $ab = e$

$= eb$

$= b$

$\Rightarrow b' = b$

Now e is called the identity w.r.t.

& b in (3) is called the inverse of a w.r.t.

and write $b = a^{-1}$.

Def $(G, \cdot)$ is a group. $(G, \cdot)$ is abelian or commutative if

abelian or commutative iff

$ab = ba$ $\forall a, b \in G$.

Ex: $GL(n, \mathbb{F})$ is noncommutative group (infinitely groups) for $n > 1$

$n = 1$, $GL(1, \mathbb{F}) = \mathbb{F}^*$, commutative

Ex: S set, $G = \mathcal{F}(S, \mathbb{R})$

$+ : G \times G \to G$ by

$+(f, g) = f + g$

$f + g : S \to \mathbb{R}$ defined by

$(f+g)(s) = f(s) + g(s)$

$0 : S \to \mathbb{R}$ $0(s) = 0$ $\forall s \in S$

is called the zero function

Note (1) $(f+g)+h = f+(g+h)$ also.

(2) $f + 0 = f = 0 + f$ for each $f \in G$

(3) For each $f \in G = \mathcal{F}(S, \mathbb{R})$

Note is $g \in G$

s.t. $f + g = 0 = g + f$

s.t. $f+g=0=g+f$

g is denoted by $-f$

$G=\mathcal{F}(S,\mathbb{R})$ is a group under addition

It is commutative:

$f+g=g+f$.

Ex. $G=\mathcal{F}(S, GL(n,\mathbb{F}))$, $n>1$

= matrix valued functions on S

$f,g: S \to GL(n,\mathbb{F})$

$(fg): S \to GL(n,\mathbb{F})$

by $(fg)(s) = f(s)\,g(s)$

then $\mathcal{F}(S, GL(n,\mathbb{F}))$, $n>1$

is a noncommutative group

Ex $O(n,\mathbb{R}) = \{ A \in GL(n,\mathbb{R}) : AA^t = I_n = A^tA \}$

$A^{-1} = A^t$ }

the set of orthogonal matrices

the set of orthogonal matrices $n \times n$

$A, B \in O(n, \mathbb{R}) \subseteq GL(n, \mathbb{R})$

$\Rightarrow AB \in O(n, \mathbb{R})$ &

$O(n, \mathbb{R})$ is a group under product

$A^{-1} = A^t$, $B^{-1} = B^t$

$(AB)^{-1} = B^{-1} A^{-1} = B^t A^t$

$= (AB)^t$