Lecture 2

Recall,

An operation is 'any' rule which assigns to each ordered pair of elements of A a unique element in A.

Properties of operation

- $a * b$ is defined for every ordered pair $(a,b)$ of element of A
- $a * b$ is uniquely defined
- If $a, b \in A$, then $a * b \in A$.

Commutative operation: $a * b = b * a \quad \forall a, b \in A$.

Associative operation: $a * (b * c) = (a * b) * c \quad \forall a, b, c \in A$

Identity element $e \in A$: $a * e = e * a = a \quad \forall a \in A$

Inverse element $a^{-1}$ ($\in A$): $a * a^{-1} = e = a^{-1} * a \quad \forall a \in A$

Ex. $x * y = x + y + 1$ operation

commutative ✓

$(x * y) * z = x + y + 1 + z + 1$

$x * (y * z) = x + y + z + 1 + 1$

associative ✓

$x * e = x$

$x + e + 1 = x$

identity $e = -1$ ✓

inverse $x * y = e$

$x + y + 1 = -1$

$y = -x - 2$ ✓

$\therefore x + y + z > 0$

$x > -y$

$x * y = |x + y|$

commutative ✓

$(x * y) * z = ||x+y| + z| = |x+y+z| \quad x+y > 0$

$|-x-y+z| \quad x+y < 0$

$x * (y * z) = |x + |y+z||$

$|x+y+z| \quad y+z > 0$

$|x-y-z| \quad y+z < 0$

Simplest & most basic of all algebraic structures is the group.

Group $(A, *)$ satisfying
set & operation

(A1) $*$ is associative
(A2) There is an element $e$ in $G$ s.t $a * e = a$ & $e * a = a$ for every element $a$ in $G$.
(A3) For every element $a \in G$, $\exists\, a^{-1} \in G$ s.t $a * a^{-1} = e = a^{-1} * a$.

$\langle G, * \rangle$

Ex.

① $\langle \mathbb{Z}, + \rangle$

② $\langle \mathbb{Q}, + \rangle$

③ $\langle \mathbb{R}, + \rangle$

④ $\langle \mathbb{Q}^*, \cdot \rangle$ , $\langle \mathbb{Q}^+, \cdot \rangle$

⑤ $\langle \mathbb{R}^*, \cdot \rangle$ $\langle \mathbb{R}^+, \cdot \rangle$

Matrices

$M_n(\mathbb{R}) = \{ n \times n$ matrices with entries in $\mathbb{R} \}$

$\langle M_n(\mathbb{R}), + \rangle$

$\langle M_n(\mathbb{R}), \cdot \rangle$ inverse absent in general.

$GL_n(\mathbb{R}) = \{ A \in M_n(\mathbb{R}) : A$ is invertible$\}$.

$\langle GL_n(\mathbb{R}), \cdot \rangle \rightarrow$ not commutative

Finite groups $\rightarrow$ in applications things are finite

Integers mod n:

Ex. $\{0, 1, 2, 3, 4, 5\}$

$a+b \mod 6$

Divide $a+b$ by 6 & take the remainder.

ignore multiples of 6 & only take the ".

$2+5 \mod 6 = 1$

closed.

$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

$a + b \mod n$

used the fact that you can always divide 2 integers to obtain a quotient & a remainder.

(Division Algorithm)

Let $a$ & $b$ be integers with $n > 0$. Then $\exists!$ integers $q$ & $r$ with the property that

$$a = bq + r, \text{ where } 0 \leq r < b.$$

Pf: Existence

Uniqueness

Existence:

$$S = \{a - bk \mid k \in \mathbb{Z} \ \& \ a - bk \geq 0\}$$

if $0 \in S$, then $b \mid a$

& $q = a/b$

$r = 0$

$0 \notin S$, Since $S \neq \emptyset$

$\{$ if $a > 0$, $a - b \cdot 0 \in S$

$a < 0$, $a - b(2a) = a(1 - 2b) \in S$ ; $a \neq 0$ & $0 \notin S \}$

Apply well-ordering to conclude

$S$ has a smallest no.

$r = a - bq$

$r < b$

if $r \geq b$ $\quad a - b(q+1)$

$= a - bq - b$

$r - b \geq 0$

$a - b(q+1) \in S$

$< a - bq$

is smaller

Using Division Algorithm,

Fix $n \in \mathbb{Z}$, then any $a \in \mathbb{Z}$ determines a unique element of $\mathbb{Z}_n$.

~~$a \equiv b \mod n$~~

Defn: $a, n \in \mathbb{Z}$ $\quad a = nq + r$

$r : [a]_n$ remainder of $a \mod n$

$a \equiv b \mod n$ iff $n \mid a - b$

$[a]_n = [b]_n$

i.e. same remainder

Ex. 19 & 7 :

$19 \equiv 7 \mod 3$

Def$^n$: $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

$a + b \mod n$

$[a+b]_n$

Really saying here is that the elements of $\mathbb{Z}_n$ are not really integers per se, but families of integers, all of which have same remainder.

equivalence class

$a = qn + [a]_n$

$b = pn + [b]_n$

$a - b =$

$(\mathbb{Z}_n, +)$

associativity:

$(a +_n b) +_n c$

$[a]_n = [b]_n$

$n \mid a-b$